On the Distribution of Frobenius of Weight 2 Eigenforms with Quadratic Coefficient Field

Jasper Van Hirtum

January 14, 2016

Abstract

In this article we present a heuristic model that describes the asymptotic behaviour of the number of primes p such that the p-th coefficient of a given eigenform is a rational integer. We treat the case of a weight 2 eigenform with quadratic coefficient field without inner twists. Moreover we present numerical data which agrees with our model and the assumptions we made to obtain it.

1 Introduction

Let f be a weight 2 cuspidal Hecke eigenform of level $\Gamma_1(N)$ with quadratic coefficient field and without inner twist. Denote the p-th coefficient of the standard q-expansion of f by $a_p(f)$. Then the set of primes $\{p \mid a_p(f) \in \mathbb{Q}\}$ is known to be of density zero, cf. [8, Corollary 1.1]. Part of the conjecture that Kumar Murty posed based on earlier work of S. Lang and H. Trotter [10] is the following.

Conjecture 1.1 (Conjecture 3.4 [12]). *Let f be a weight 2 normalized cuspidal Hecke eigenform of level $\Gamma_1(N)$ with quadratic coefficient field and without inner twists. Then*

$$\#\{p < x \text{ prime} \mid a_p(f) \in \mathbb{Q}\} \sim c_f \frac{\sqrt{x}}{\log x},$$

with c_f a constant that depends on the eigenform.

In this paper we present a heuristic model that makes this conjecture explicit. More precisely we will prove the following theorem.

Theorem 6.3. *Let f be a weight 2 normalized cuspidal Hecke eigenform of level $\Gamma_1(N)$ with quadratic coefficient field $\mathbb{Q}(\sqrt{D})$ and without inner twists. Assume that there exists a positive integer m_0 such that Assumptions 4.4 and 3.1 hold for f and all positive integers in $m_0\mathbb{Z}$. Then there is an explicit constant $\widehat{F}$, depending on the images of the Galois representations attached to f, such that Conjecture 1.1 holds with*

$$c_f = \frac{16\sqrt{D}\widehat{F}}{3\pi^2}.$$

Our work is based on the methods used by Serge Lang and Hale Trotter in [10] where they derive a heuristic model for the behaviour of the of the coefficients of the L-polynomial of an elliptic curve, i.e., the coefficients of a weight 2 eigenform with rational coefficients.

Section 2 contains some facts concerning modular forms. In Section 3 we describe the assumptions needed to reduce our problem to the product of two functions: one concerning the real absolute value and the other derived from the non-archimedean places. In Section 4 we will discuss the factor of the infinite place. For this factor we will use recent results on the Sato-Tate conjecture for abelian surfaces and one additional assumption. The factor at the finite places will be discussed in Section 5. We will derive this factor from the adelic representation attached to the eigenform. Section 6 contains the proof of our main result. In the final section we compare our model to numerical data. Moreover we check all assumptions and intermediate results numerically. All computations agree with our model and the assumptions we made to obtain these results. Therefore we are led to believe our heuristic model correctly predicts the asymptotic number of primes with rational integer coefficient.

Remark 1.2. *Let f be a cuspidal Hecke eigenform of level $\Gamma_1(N)$.*

1. *If f has CM by the Dirichlet character χ, then $\chi(p)a_p(f) = a_p(f)$ for almost all primes. If p is a prime such that $\chi(p) \neq 1, 0$ then $a_p(f) = 0$. By Dirichlet's theorem of arithmetic progression the density of the set $\{p \text{ prime } | a_p(f) = 0\}$ is at least $\frac{1}{2}$.*

2. *Suppose that f has quadratic coefficient field K_f and an inner twist by the Dirichlet character χ and non-trivial automorphism $\sigma \in Gal(K_f/\mathbb{Q})$. Let p be a prime such that $\chi(p) = 1$ then $\sigma(a_p(f)) = \chi(p) \cdot a_p(f) = a_p(f)$ so $a_p(f) \in \mathbb{Q}$. If n is the modulus of the character χ and p is a prime such that $p \equiv 1 \mod n$, then $\chi(p) = 1$ and $a_p(f) \in \mathbb{Q}$. Again by Dirichlet's theorem of arithmetic progression the density of the set $\{p \text{ prime } | a_p(f) \in \mathbb{Q}\}$ is at least $\frac{1}{\phi(n)}$.*

3. *Let f be a weight k form without inner twists and let d be the extension degree of K_f over $\mathbb{Q}$. Then Kumar Murty conjectured the following [12, Conjecture 3.4]*

$$\#\{p < x \text{ prime } \mid a_p(f) \in \mathbb{Q}\} \sim c_f \begin{cases} \sqrt{x}/\log x & \text{if } k = d = 2, \\ \log\log x & \text{if } k = 2 \text{ and } d = 3, \\ & \text{or } k = 3 \text{ and } d = 2, \\ 1 & \text{else.} \end{cases}$$

Acknowledgements

I wish to express my sincere gratitude to Jan Tuitman and Gabor Wiese for suggesting me this problem, for our discussions, for their enthusiasm and for their guidance.

I would also like to thank Andrew Sutherland and the anonymous referee for useful comments.

2 Preliminaries

In this section we some recall basic facts concerning modular forms.

Lemma 2.1. *Let f be a weight 2 eigenform of level $\Gamma_1(N)$ and trivial nebentypus. If N is square-free, then f does not have inner twists.*

Proof. This follows from [15, Theorem 3.9 bis]. □

Lemma 2.2. *Let f be a normalized cuspidal Hecke eigenform of level $\Gamma_1(N)$.*

1. *If f has trivial nebentypus, then the coefficient field of f is totally real.*
2. *If f does not have any inner twist, then f has trivial nebentypus.*

Proof. Let K_f be the coefficient field of f, N the level and ε the nebentypus of f. Let $< \cdot, \cdot >$ be the Petersson scalar product. The Hecke operators are self adjoint with respect to $< \cdot, \cdot >$ up to the character ε [9, Theorem 5.1], i.e.,

$$< T_p \cdot, \cdot >= \varepsilon(p) < \cdot, T_p \cdot >,$$

for all primes p not dividing N. Hence for any such prime p we obtain

$$\begin{aligned} a_p(f) < f, f > &=< T_p f, f > \\ &= \varepsilon(p) < f, T_p f > \\ &= \varepsilon(p)\widehat{a_p(f)} < f, f >, \end{aligned}$$

where $\widehat{a_p(f)}$ denotes the complex conjugate of $a_p(f)$. In particular

$$\varepsilon^{-1}(p) a_p(f) = \widehat{a_p(f)},$$

for all primes p not dividing N.

1. If the nebentypus of f is trivial, then by the above

$$a_p(f) = \widehat{a_p(f)}$$

for all primes p not dividing N. In particular $K_f \subset \mathbb{R}$.

2. Note that $\widehat{\cdot}|_{K_f} \in \mathrm{Aut}_{\mathbb{Q}}(K_f)$ so if ε is not the trivial character, then f has inner twist by ε^{-1}.

$\square$

3 Heuristic model

For the remainder of this article f will be a normalized cuspidal Hecke eigenform of weight 2 and level $\Gamma_1(N)$ without inner twist or CM and with quadratic coefficient field K_f. By Lemma 2.2 $K_f \subset \mathbb{R}$ and f has trivial nebentypus. Let D be the positive square-free integer such that $K_f = \mathbb{Q}(\sqrt{D})$. Denote by $\overline{\cdot}$ the unique non-trivial element of the Galois group of $K_f/\mathbb{Q}$. Define

$$Z_p := a_p(f) - \overline{a_p(f)}.$$

Note that $Z_p \in \sqrt{D}\mathbb{Z}$ since $a_p(f)$ is an algebraic integer in K_f. Moreover

$$\begin{aligned} a_p(f) \in \mathbb{Q} &\Leftrightarrow Z_p = 0 \\ &\Leftrightarrow \frac{-m\sqrt{D}}{2} < Z_p < \frac{m\sqrt{D}}{2} \text{ and } Z_p \equiv 0 \mod m\sqrt{D}\mathbb{Z} \text{ for all } m \in \mathbb{N}. \end{aligned}$$

In other words the condition $a_p(f) \in \mathbb{Q}$ is equivalent to a condition on the real and ℓ-adic absolute value of Z_p for finite places ℓ dividing m for any positive integer m. Denote $\pi(x) := \#\{p < x \text{ prime}\}$ and

$$\begin{aligned} P(x) &:= \frac{\#\{p < x \text{ prime} \mid Z_p = 0\}}{\pi(x)}, \\ P_m(x) &:= \frac{\#\{p < x \text{ prime} \mid Z_p \equiv 0 \mod m\sqrt{D}\mathbb{Z}\}}{\pi(x)}, \\ P^m(x) &:= \frac{\#\{p < x \text{ prime} \mid Z_p \in]\frac{-m\sqrt{D}}{2}, \frac{m\sqrt{D}}{2}[\}}{\pi(x)}. \end{aligned}$$

Since $|a_p(f)| = \mathcal{O}(\sqrt{p})$ cf. [9, Lemma 2]

$$\lim_{m\to\infty} P_m(x) = P(x) \text{ and } \lim_{m\to\infty} P^m(x) = 1$$

for all $x > 2$. In particular

$$\lim_{m\to\infty} \frac{P^m(x) \cdot P_m(x)}{P(x)} = 1 \quad \text{for all } x > 2$$

so

$$\lim_{x\to\infty} \lim_{m\to\infty} \frac{P^m(x) \cdot P_m(x)}{P(x)} = 1.$$

Our first assumption states that the order of the double limit can be reversed.

Assumption 3.1. *Let f be as above. Then*

$$\lim_{m\to|\infty} \lim_{x\to\infty} \frac{P^m(x) \cdot P_m(x)}{P(x)} = 1,$$

where $\lim_{m\to|\infty}$ denotes that the limit over m is taken by divisibility.

We say that a is the limit of a series $\{a_m\}_{\mathbb{N}}$ by divisibility if for all $\varepsilon > 0$ there exists a positive integer m_0 such that for all $m \in m_0\mathbb{N}$

$$|a_m - a| < \varepsilon.$$

In Section 6 we will show that the convergence of the double limit in Assumption 3.1 follows from the weaker condition that there exists at least one positive integer m satisfying the following assumption.

Assumption 3.2. *Let f be as above and m a positive integer. Then*

$$\lim_{x\to\infty} \frac{P^m(x) \cdot P_m(x)}{P(x)} = \alpha_m,$$

with $0 < \alpha_m < \infty$.

Note that the $0 < \alpha_m$ part of the statement will follow immediately from Lemma 5.1. Assumption 3.2 is enough to prove the asymptotic behaviour of $\#\{p < x \text{ prime} \mid a_p \in \mathbb{Q}\}$. However to make the constant c_f explicit we will need the stronger Assumption 3.1.

By deriving suitable expressions for the arithmetic part $P_m(x)$ and the real part $P^m(x)$ respectively we will obtain the asymptotic behaviour of $P(x)$ predicted by Conjecture 1.1 from Assumption 3.2. Additionally under the stronger condition of Assumption 3.1 we will obtain an explicit constant. In Section 5 we use Chebotarev's density theorem to prove an explicit formula for the factor $P_m(x)$. For the factor at the infinite place we will need additional assumptions. We describe the assumptions and the results that follow in the next section.

4 The place at infinity

In this section we describe a heuristic formula for the factor

$$P^m(x) = \frac{\#\{p < x \text{ prime} \mid Z_p \in]\frac{-m\sqrt{D}}{2}, \frac{m\sqrt{D}}{2}[\}}{\pi(x)},$$

which we derive from natural assumptions. We use results from a recent paper by F. Fité, K. Kedlaya, V. Rotger and A. Sutherland that describes the joint distribution of the coefficients of the normalized L_p-polynomial of hyperelliptic curves of genus 2 under the assumption of the Sato-Tate conjecture for abelian varieties (cf. [5]). Note that we use the Sato-Tate conjecture for abelian varieties rather than the proven Sato-Tate distribution for modular forms. The latter describes the distribution of the real absolute value of the coefficients but claims nothing about the coefficients as elements of the number field K_f.

Let f be as above. Then one can associate via Shimura's construction (cf. [4, section 1.7]) an abelian variety $\mathcal{A}_f$ of dimension $[K_f : \mathbb{Q}]$ to the eigenform f. For every prime p the L_p-polynomial associated to the variety $\mathcal{A}_f$ splits as the L_p-polynomial of the eigenform and its Galois conjugate over K_f. More precisely, let $L_p(T) := p^2T^4 + pX_pT^3 + Y_pT^2 + X_pT + 1$ be the L_p-polynomial of $\mathcal{A}_f$ then

$$L_p(T) = (pT^2 - a_p(f)T + 1)(pT^2 - \overline{a_p(f)}T + 1).$$

Hence

$$a_p(f) = -\frac{X_p}{2} \pm \sqrt{2p - Y_p + \frac{X_p^2}{4}}.$$

Note that from the L_p-polynomial of $\mathcal{A}_f$ we cannot deduce $a_p(f)$ completely. Indeed we only obtain its Galois orbit. However we can decide whether or not Z_p lies in a symmetrical interval around zero since

$$|Z_p| = \sqrt{8p - 4Y_p + X_p^2}.$$

Let $a_{1,p} = \frac{X_p}{\sqrt{p}}$ and $a_{2,p} = \frac{Y_p}{p}$ be the coefficients of the normalized L_p-polynomial $L_p(T/\sqrt{p})$. Then

$$Z_p \in \left] -\frac{m\sqrt{D}}{2}, \frac{m\sqrt{D}}{2} \right[\Leftrightarrow \sqrt{2 - a_{2,p} + a_{1,p}^2/4} < \frac{m\sqrt{D}}{4\sqrt{p}}.$$

The generalized Sato-Tate conjecture states that this distribution is completely determined by the so called Sato-Tate group. In [5] Fité et al. study the joint distribution of $(a_{1,p}, a_{2,p})$ for abelian surfaces. More precisely they prove the following theorem.

Theorem 4.1. *Let $\mathcal{A}$ be an abelian surface. There exist exactly 52 Sato-Tate groups for abelian surfaces, of which only 34 occur over $\mathbb{Q}$. Moreover the conjugacy class of the Sato-Tate group of $\mathcal{A}$ is uniquely determined by its Galois type (cf. [5, Def. 1.3]) and vice versa.*

Proof. This is Theorem 1.4 in [5]. □

Corollary 4.2. *Let f and $\mathcal{A}_f$ be as above. The generalized Sato-Tate conjecture holds for A_f and the joint distribution of $(a_{1,p}, a_{2,p})$ is given by*

$$\Phi : T \to \mathbb{R} : (x,y) \mapsto \frac{1}{2\pi^2}\sqrt{\frac{(y-2x+2)(y+2x+2)}{x^2-4y+8}},$$

where T is the subset of the plane (Fig. 1)

$$T := \left\{(x,y) | \, y+2 > |2x| \text{ and } 4y < x^2+8\right\}.$$

Moreover denote by δ the measure with density Φ and let S be a measurable set. Then

$$\delta(S) \sim \frac{\#\{p < x \text{ prime} \mid (a_{1,p}, a_{2,p}) \in S\}}{\pi(x)}.$$

Proof. The $\mathbb{Q}$-algebra of endomorphisms of $\mathcal{A}_f$ over $\mathbb{Q}$ is K_f. Moreover the $\mathbb{Q}$-algebra of endomorphisms of $\mathcal{A}_f$ over $\overline{\mathbb{Q}}$ is also K_f since f does not have any inner twists (cf. [13, Theorem 5]). So all endomorphisms of $\mathcal{A}_f$ over $\overline{\mathbb{Q}}$ are already defined over $\mathbb{Q}$. In particular the Galois type of $\mathcal{A}_f$ is

$$[\mathrm{Gal}(\mathbb{Q}/\mathbb{Q}), K_f \otimes_{\mathbb{Z}} \mathbb{R}] = [1, \mathbb{R} \times \mathbb{R}],$$

since K_f is a real quadratic number field. The generalized Sato-Tate conjecture is proven for abelian surfaces of this Galois type by Christian Johansson in [6][Proposition 22]. It follows from Tables 8 and 11 in [5] that the Sato-Tate group of $\mathcal{A}_f$ is $SU(2) \times SU(2)$. Finally, the joint distribution function of this group is given by [5, Table 5]. □

The following result is proven by K. Koo, W. Stein and G. Wiese (cf. [8, Corollary 1.1]). We give an alternative proof using recent results on Sato-Tate equidistribution.

Corollary 4.3. *Let f be as above. The set $\{p < x \text{ prime} \mid a_p(f) \in \mathbb{Q}\}$ has density zero.*

Proof. Let $S = \{(x,y) \mid \sqrt{x^2-4y+8} = 0\}$ then by Corollary 4.2

$$\frac{\#\{p < x \text{ prime} \mid a_p(f) \in \mathbb{Q}\}}{\pi(x)} = \frac{\#\{p < x \text{ prime} \mid (a_{1,p}, a_{2,p}) \in S\}}{\pi(x)} \sim \delta(S).$$

Clearly, $\delta(S) = 0$. □

Define for any $\varepsilon > 0$

$$T_\varepsilon := \left\{(x,y) \in T \mid \sqrt{x^2/4 - y + 2} < \varepsilon\right\}.$$

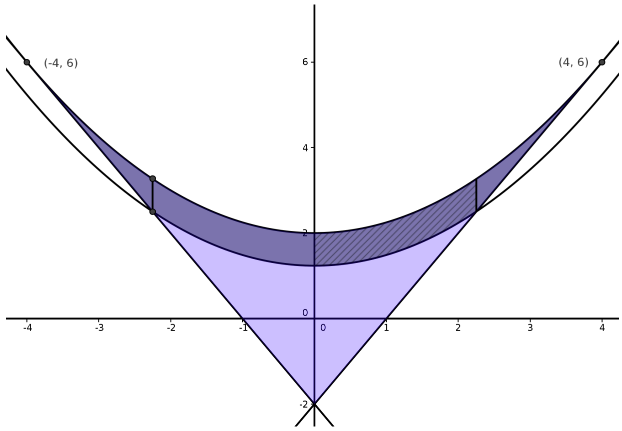


Figure 1: The areas T (dark and light blue), T_ε (dark blue) and T_ε^1 (hatched).

Then

$$Z_p \in \left] -\frac{m\sqrt{D}}{2}, \frac{m\sqrt{D}}{2} \right[\Leftrightarrow (a_{1,p}, a_{2,p}) \in T_{m\sqrt{D}/(4\sqrt{p})}.$$

By Corollary 4.2

$$\delta(T_{m\sqrt{D}/(4\sqrt{p})}) \sim \frac{\#\left\{q < x \text{ prime} \mid \sqrt{2 - a_{2,q} + a_{1,q}^2/4} < \frac{m\sqrt{D}}{4\sqrt{p}}\right\}}{\pi(x)}$$

since $T_{m\sqrt{D}/(4\sqrt{p})}$ is a measurable set. We will need the following heuristic assumption.

Assumption 4.4. *Let m be a positive integer. Then*

$$P^m(x) \sim \frac{1}{\pi(x)} \sum_{p=2}^{x} \delta(T_{m\sqrt{D}/(4\sqrt{p})})$$

where the sum is taken only over primes.

The idea behind this assumption is that approximating the probability of $\left|\frac{Z_p}{2\sqrt{p}}\right| < \frac{m\sqrt{D}}{4\sqrt{p}}$ (which is either 1 or 0) by the probability that $\left|\frac{Z_q}{2\sqrt{q}}\right| < \frac{m\sqrt{D}}{4\sqrt{p}}$ for any prime q is 'good on average'. Note that for each individual prime p this approximation is bad. However the assumption states that summing over all primes p does yield a good approximation.

Lemma 4.5. *The measure of the set T_ε is*

$$\delta(T_\varepsilon) = \frac{32}{3\pi^2}\varepsilon + o(\varepsilon).$$

Proof. It suffices to bound the integral

$$\delta(T_\varepsilon) = \int_{T_\varepsilon} \Phi \, \mathrm{d}A.$$

Since the density function Φ is even with respect to the first variable x we can restrict to positive x. We split the integration domain T_ε in two parts (Fig. 1)

$$\begin{aligned} T_\varepsilon^1 &:= \{(x,y) \in T_\varepsilon \mid 0 < x < 4 - 2\varepsilon\} \text{ and} \\ T_\varepsilon^2 &:= \{(x,y) \in T_\varepsilon \mid 4 - 2\varepsilon < x < 4\}. \end{aligned}$$

So

$$\delta(T_\varepsilon) = 2\int_{T_\varepsilon^1} \Phi \, \mathrm{d}A + 2\int_{T_\varepsilon^2} \Phi \, \mathrm{d}A.$$

Parametrizations of both sets are given respectively by

$$\begin{aligned} T_\varepsilon^1 &= \{(u, u^2/4 + 2 - v^2) \mid 0 < u < 4 - 2\varepsilon \ \wedge \ 0 < v < \varepsilon\} \text{ and} \\ T_\varepsilon^2 &= \{(u, u^2/4 + 2 - v^2) \mid 4 - 2\varepsilon < u < 4 \ \wedge \ 0 < v < 2 - u/2\}. \end{aligned}$$

The determinant of the Jacobian of the parametrization, $\mathrm{d}A$, is $2v \, \mathrm{d}v \, \mathrm{d}u$ so

$$\begin{aligned} &2\Phi(u, u^2/4 + 2 - v^2) \, \mathrm{d}A \\ &= \frac{2}{2\pi^2} \sqrt{\frac{(u^2/4 + 2 - v^2 - 2u + 2)(u^2/4 + 2 - v^2 + 2u + 2)}{u^2 - u^2 - 8 + 4v^2 + 8}} 2v \, \mathrm{d}v \, \mathrm{d}u \\ &= \frac{1}{4\pi^2} \sqrt{(u^2 + 16 - 4v^2 - 8u)(u^2 + 16 - 4v^2 + 8u)} \, \mathrm{d}v \, \mathrm{d}u \\ &= \frac{1}{4\pi^2} \sqrt{(u^2 + 16 - 4v^2)^2 - 64u^2} \, \mathrm{d}v \, \mathrm{d}u. \end{aligned}$$

First we show that

$$2\int_{T_\varepsilon^2} \Phi \, \mathrm{d}A = \mathcal{O}(\varepsilon^2).$$

It suffices to show that the limit of $\frac{1}{\varepsilon^2} 2 \int_{T_\varepsilon^2} \Phi \, \mathrm{d}A$ is finite if ε tends to zero. Let us compute

$$\lim_{\varepsilon \to 0} \frac{1}{\varepsilon^2} 2 \int_{T_\varepsilon^2} \Phi \, \mathrm{d}A = \lim_{\varepsilon \to 0} \frac{1}{\varepsilon^2} \frac{1}{4\pi^2} \int_{4-2\varepsilon}^{4} \int_0^{2-u/2} \sqrt{(u^2 + 16 - 4v^2)^2 - 64u^2} \, \mathrm{d}v \, \mathrm{d}u.$$

Then by l'Hôpital's rule we obtain

$$\begin{aligned} \lim_{\varepsilon \to 0} \frac{1}{\varepsilon^2} 2 \int_{T_\varepsilon^2} \Phi \, \mathrm{d}A &\overset{\widehat{\mathrm{H}}}{=} \lim_{\varepsilon \to 0} \frac{1}{\varepsilon} \frac{1}{2\pi^2} \int_0^\varepsilon \sqrt{(\varepsilon^2 + 16 - 4v^2)^2 - 64\varepsilon^2} \, \mathrm{d}v \\ &< \lim_{\varepsilon \to 0} \frac{1}{\varepsilon} \frac{1}{2\pi^2} \int_0^\varepsilon \sqrt{(\varepsilon^2 + 16)^2 - 64\varepsilon^2} \, \mathrm{d}v \\ &= \lim_{\varepsilon \to 0} \frac{1}{2\pi^2} \sqrt{(\varepsilon^2 + 16)^2 - 64\varepsilon^2} \\ &= \frac{8}{\pi^2} < \infty. \end{aligned}$$

In particular we obtain

$$\delta(T_\varepsilon) = 2\int_{T_\varepsilon^1} \Phi \,\mathrm{d}A + \mathcal{O}(\varepsilon^2).$$

Finally, denote $\phi(u,v) = 2\Phi\frac{\mathrm{d}A}{\mathrm{d}v\,\mathrm{d}u} = \frac{1}{4\pi^2}\sqrt{(u^2+16-4v^2)^2-64u^2}$. Then, again by l'Hôpital's rule and Leibniz rule for double integration

$$\begin{aligned}
\lim_{\varepsilon\to 0}\frac{\frac{32}{3\pi^2}\varepsilon - \delta(T_\epsilon)}{\varepsilon} &= \lim_{\varepsilon\to 0}\frac{1}{\varepsilon}\left(\frac{32}{3\pi^2}\varepsilon - \int_0^{4-2\varepsilon}\int_0^{\varepsilon}\phi(u,v)\,\mathrm{d}v\,\mathrm{d}u\right)\\
&\overset{\widehat{\mathrm{H}}}{=} \lim_{\varepsilon\to 0}\frac{32}{3\pi^2} - \int_0^{4-2\varepsilon}\phi(u,\varepsilon)\,\mathrm{d}u + 2\int_0^{\varepsilon}\phi(4-2\varepsilon,v)\,\mathrm{d}v\\
&= \frac{32}{3\pi^2} - \int_0^4 \phi(u,0)\,\mathrm{d}u + 0\\
&= \frac{32}{3\pi^2} - \frac{1}{4\pi^2}\int_0^4 \sqrt{(u^2+16)^2-64u^2}\,\mathrm{d}u\\
&= \frac{32}{3\pi^2} - \frac{1}{4\pi^2}\int_0^4 (16-u^2)\,\mathrm{d}u\\
&= \frac{32}{3\pi^2} - \frac{1}{4\pi^2}\left[16u - \frac{u^3}{3}\right]_0^4\\
&= 0.
\end{aligned}$$

□

Corollary 4.6. *For all $m > 0$ satisfying Assumption 4.4*

$$P^m(x) \sim \frac{16m\sqrt{D}}{3\pi^2\sqrt{x}}.$$

Proof. By Assumption 4.4, Lemma 4.5 with $\varepsilon = m\sqrt{D}/(4\sqrt{p})$ and the fact that $\sum_{p=2}^{x}\frac{1}{2\sqrt{p}} \sim \frac{\sqrt{x}}{\log x}$ respectively we obtain

$$\begin{aligned}
P^m(x) &\sim \frac{1}{\pi(x)}\sum_{p=2}^{x}\delta(T_{m\sqrt{D}/(4\sqrt{p})})\\
&\sim \frac{1}{\pi(x)}\frac{16m\sqrt{D}}{3\pi^2}\sum_{p=2}^{x}\frac{1}{2\sqrt{p}}\\
&\sim \frac{16m\sqrt{D}}{3\pi^2}\frac{\sqrt{x}}{\pi(x)\log x}\\
&\sim \frac{16m\sqrt{D}}{3\pi^2\sqrt{x}}.
\end{aligned}$$

□

5 Finite places

In this section we describe the remaining factor $P_m(x)$. No heuristic is needed to obtain the results of this section. For each positive integer m the factor P_m can be computed by Chebotarev's density theorem and the image of the mod m Galois representation attached to f.

Let f be as above and denote the ring of integers of its coefficient field by $\mathcal{O}_f$. Let m be a positive integer and denote $\mathcal{O}_m := \mathcal{O}_f \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$. Denote the absolute Galois group of $\mathbb{Q}$ by $G_{\mathbb{Q}}$. Then the action of $G_{\mathbb{Q}}$ on the m-torsion points of $\mathcal{A}_f$ induces a mod-m representation

$$\rho_m : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_m).$$

By taking the inverse limit over all integers m we obtain an adelic representation

$$\widehat{\rho} := \varprojlim_m \rho_m : G_{\mathbb{Q}} \to GL_2(\widehat{\mathcal{O}}),$$

where $\widehat{\mathcal{O}} = \mathcal{O}_f \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ is the ring of finite adeles of K_f. If ℓ is a prime we obtain an ℓ-adic representation by taking the limit over all powers of ℓ torsion points

$$\widehat{\rho}_\ell := \varprojlim_k \rho_{\ell^k} : G_{\mathbb{Q}} \to GL_2(\widehat{\mathcal{O}}_\ell),$$

with $\widehat{\mathcal{O}}_\ell = \mathcal{O}_f \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Note that by definition $\widehat{\rho} = \prod_\ell \widehat{\rho}_\ell$. Moreover for any positive integer m and any prime ℓ dividing m the following diagram commutes

$$\begin{tikzcd}
 & G_{\mathbb{Q}} \arrow[ddl, "\widehat{\rho}_\ell"'] \arrow[d, "\widehat{\rho}"] \arrow[ddr, "\rho_m"] & \\
 & GL_2(\widehat{\mathcal{O}}) \arrow[dl] \arrow[d] \arrow[dr] & \\
GL_2(\widehat{\mathcal{O}}_\ell) \arrow[r] & GL_2(\mathcal{O}_\ell) & GL_2(\mathcal{O}_m). \arrow[l]
\end{tikzcd}$$

Let $\overline{\cdot}$ be the unique non-trivial element of the Galois group of K_f over $\mathbb{Q}$. Then $\overline{\cdot}$ induces by the tensor product endomorphisms on $\widehat{\mathcal{O}}$, $\widehat{\mathcal{O}}_\ell$ and $\mathcal{O}_m$. By abuse of notation we denote each of these morphisms by $\overline{\cdot}$. Hence we obtain the following maps

$$Z : GL_2(\widehat{\mathcal{O}}) \to \widehat{\mathcal{O}} : \sigma \mapsto \operatorname{tr}\sigma - \overline{\operatorname{tr}\sigma},$$
$$Z : GL_2(\widehat{\mathcal{O}}_\ell) \to \widehat{\mathcal{O}}_\ell : \sigma \mapsto \operatorname{tr}\sigma - \overline{\operatorname{tr}\sigma} \quad \text{and}$$
$$Z : GL_2(\mathcal{O}_m) \to \mathcal{O}_m : \sigma \mapsto \operatorname{tr}\sigma - \overline{\operatorname{tr}\sigma}.$$

Consider the following (subsets) of the images of the representations

$$\begin{aligned} \widehat{\mathcal{G}} &:= \mathrm{Im}\ \widehat{\rho}, & \widehat{\mathcal{G}}^t &:= \{\sigma \in \widehat{\mathcal{G}} \mid Z(\sigma) = 0\}, \\ \widehat{\mathcal{G}}_\ell &:= \mathrm{Im}\ \widehat{\rho}_\ell, & \widehat{\mathcal{G}}^t_\ell &:= \{\sigma \in \widehat{\mathcal{G}}_\ell \mid Z(\sigma) = 0\}, \\ \mathcal{G}_m &:= \mathrm{Im}\ \rho_m, & \mathcal{G}^t_m &:= \{\sigma \in \mathcal{G}_m \mid Z(\sigma) = 0\}. \end{aligned}$$

Define for each positive integer m

$$F_m := m \frac{\#\mathcal{G}^t_m}{\#\mathcal{G}_m}.$$

Lemma 5.1. *Let m be a positive integer then*

$$P_m(x) \sim \frac{1}{m} F_m.$$

Proof. Let m be a positive integer. Then by Chebotarev's density theorem the conjugacy class of Frob_p is equidistributed in $\mathcal{G}_m$ where p varies over all primes not dividing mN, i.e., for all conjugacy class Cl of $\mathcal{G}_m$ we have

$$\#\{p < x \text{ prime } \mid p \nmid mN \text{ and } \rho_m(\mathrm{Frob}_p) \in Cl\} \sim \frac{\#Cl}{\#\mathcal{G}_m} \pi(x).$$

Denote by $\imath$ the morphism of $\mathcal{O}_f$ to $\mathcal{O}_m$ given by sending z to $z \otimes 1$. If p is a prime that does not divide mN, then $\mathrm{tr}\,(\rho_m(\mathrm{Frob}_p)) = \imath(a_p(f)) \in \mathcal{O}_m$ (cf. [3, Theorem 3.1.a]). Note that $Z(\sigma)$ only depends on the conjugacy class of the matrix σ so $Z(\rho_m(\mathrm{Frob}_p))$ is well defined. Moreover

$$\imath(Z_p) = Z(\rho_m(\mathrm{Frob}_p)) \in \mathcal{O}_m,$$

since $Z_p = a_p(f) - \overline{a_p(f)}$ by definition. In particular $Z_p \equiv 0 \mod m\sqrt{D}\mathbb{Z}$ if and only if $Z(\rho_m(\mathrm{Frob}_p)) = 0$ as an element of $\mathcal{O}_m$. Hence

$$\begin{aligned} P_m(x) &= \frac{\#\{p < x \text{ prime} \mid Z_p \equiv 0 \mod m\sqrt{D}\mathbb{Z}\}}{\pi(x)} \\ &\sim \frac{\#\{p < x \text{ prime } \mid p \nmid mN \text{ and } Z(\rho_m(\mathrm{Frob}_p)) = 0\}}{\pi(x)} \\ &\sim \frac{\#\{\sigma \in \mathcal{G}_m \mid Z(\sigma) = 0\}}{\#\mathcal{G}_m} \\ &= \frac{\#\mathcal{G}^t_m}{\#\mathcal{G}_m}. \end{aligned}$$

□

The following theorem will enable us to give explicit formulas for the cardinalities of $\mathcal{G}_{\ell^k}$ and $\{\mathcal{G}_{\ell^k} \mid Z(\sigma) = 0\}$ for almost all primes.

Define

$$\widehat{\mathcal{A}}_\ell = \{\sigma \in GL_2(\widehat{\mathcal{O}}_\ell) \mid \det \sigma \in \mathbb{Z}_\ell^\times\}.$$

Theorem 5.2 (Ribet)**.** *Let f be a weight 2 cusp form without inner twists. Then for all primes ℓ the image of the ℓ-adic representation, $\widehat{\mathcal{G}}_\ell$, is an open subgroup of $\widehat{\mathcal{A}}_\ell$. Moreover $\widehat{\mathcal{G}}_\ell = \widehat{\mathcal{A}}_\ell$ for almost all primes. We say that the prime ℓ has large image if the inclusion is an equality, and we say that ℓ is exceptional otherwise.*

Proof. This is a special case of [14, Theorem 0.1]. □

Let ℓ be a prime and k a positive integer. Define $\mathcal{A}_{\ell^k}$ be the image of $\widehat{\mathcal{A}}_\ell$ under the natural projection modulo ℓ^k and $\mathcal{A}^t_{\ell^k} = \{\sigma \in \mathcal{A}_{\ell^k} \mid Z(\sigma) = 0\}$. If ℓ is a prime with large image, then $\mathcal{A}_{\ell^k} = \mathcal{G}_{\ell^k}$ so

$$F_{\ell^k} = \ell^k \frac{\#\mathcal{A}^t_{\ell^k}}{\#\mathcal{A}_{\ell^k}}.$$

Note that $\widehat{\mathcal{O}}_\ell \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ if ℓ splits in $\mathcal{O}_f$. If ℓ is inert in $\mathcal{O}_f$ then $\widehat{\mathcal{O}}_\ell$ is the ring of integers of the unique unramified quadratic extension of $\mathbb{Q}_\ell$, denoted by $\mathbb{Z}_{\ell^2}$. In the next two sections we describe the cardinalities of $\mathcal{A}_{\ell^k}$ and $\mathcal{A}^t_{\ell^k}$ in the inert and split case respectively. For both cases we will need the following lemma and its corollary.

Lemma 5.3. *Let R be a finite local ring with maximal ideal $\mathfrak{m}$. Denote $r = \#R$ and $m = \#\mathfrak{m}$. Then*

$$\#GL_2(R) = (r^2 - m^2) \cdot r \cdot (r - m).$$

Proof. Let $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(R)$. Then

$$\sigma \in GL_2(R) \Leftrightarrow ad \not\equiv bc \mod \mathfrak{m}.$$

The vector (a, b) can be any vector not contained in $\mathfrak{m}^2$. There are $r^2 - m^2$ such vectors. We consider two cases depending on the valuation of b in R.

First, if $b \in \mathfrak{m}$, then $a \in R^\times$ so

$$\begin{aligned} ad \not\equiv bc \mod \mathfrak{m} &\Leftrightarrow d \not\equiv bca^{-1} \mod \mathfrak{m} \\ &\Leftrightarrow d \not\equiv 0 \mod \mathfrak{m}. \end{aligned}$$

Hence c can be any element of R and d any element of $R^\times$. There are $r \cdot (r - m)$ such vectors (c, d).

Second, if $b \not\in \mathfrak{m}$, then

$$ad \not\equiv bc \mod \mathfrak{m} \Leftrightarrow adb^{-1} \not\equiv c \mod \mathfrak{m}.$$

Hence d can be any element of R and c any element not contained in $adb^{-1} + \mathfrak{m}$. There are $r \cdot (r - m)$ such vectors.

In either case we obtain $r \cdot (r - m)$ possibilities for the second vector. Hence $\#GL_2(R) = (r^2 - m^2) \cdot r \cdot (r - m)$. □

Corollary 5.4. *Let ℓ be a prime and k a positive integer. Then*

$$\#GL_2(\mathbb{Z}/\ell^k\mathbb{Z}) = \ell^{4k-3}(\ell^2-1)(\ell-1).$$

5.1 Inert Primes

Let f be as above, suppose that ℓ is an odd inert prime in $\mathcal{O}_f$ the ring of integers of the coefficient field of f. Then

$$\widehat{\mathcal{O}}_\ell \cong \mathcal{O}_f \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathbb{Z}_{\ell^2}.$$

Recall that $\mathbb{Z}_{\ell^2}$ is the ring of integers of the unique unramified quadratic extension of $\mathbb{Q}_\ell$. If $\alpha \in \overline{\mathbb{Q}}$ with α^2 a square-free integer that is congruent to a quadratic non-residue modulo ℓ, then $\mathbb{Q}_\ell(\alpha)$ is an unramified quadratic extension of $\mathbb{Q}_\ell$ with ring of integers $\mathbb{Z}_\ell[\alpha]$ hence

$$\mathbb{Z}_{\ell^2} \cong \mathbb{Z}_\ell[\alpha].$$

Moreover the morphism $\overline{\cdot}$ is given by

$$\overline{\cdot} : \mathbb{Z}_\ell[\alpha] \to \mathbb{Z}_\ell[\alpha] : a + \alpha b \mapsto a - \alpha b.$$

If ℓ is an inert prime in $\mathcal{O}_f$, then we can take $\alpha = \sqrt{D}$ with D the square-free integer such that $K_f = \mathbb{Q}(\sqrt{D})$. If moreover the ℓ-adic representation attached to f has large image in the sense of Theorem 5.2 the sets $\mathcal{G}_{\ell^k}$ and $\{\sigma \in \mathcal{G}_{\ell^k} \mid Z(\sigma) = 0\}$ are respectively

$$\begin{aligned}
\mathcal{A}_{\ell^k,I} &:= \left\{\sigma \in GL_2(\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]) \mid \det\sigma \in \mathbb{Z}/\ell^k\mathbb{Z}^\times\right\} \text{ and} \\
\mathcal{A}^t_{\ell^k,I} &:= \left\{\sigma \in GL_2(\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]) \mid \det\sigma \in \mathbb{Z}/\ell^k\mathbb{Z}^\times \wedge \ \operatorname{tr}\sigma \in \mathbb{Z}/\ell^k\mathbb{Z}\right\}.
\end{aligned}$$

Proposition 5.5. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#\mathcal{A}_{\ell^k,I} = \ell^{7k-5}(\ell^4-1)(\ell-1).$$

Proof. There are $(\ell^2-1)\ell^{2k-2}$ units $\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$, of which $(\ell-1)\ell^{k-1}$ units are embedded in $\mathbb{Z}/\ell^k\mathbb{Z}$. By Lemma 5.3

$$\#GL_2(\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]) = \ell^{8k-6}(\ell^4-1)(\ell^2-1).$$

Since any unit occurs equally many times as the determinant of a matrix in $GL_2(\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha])$ we obtain

$$\begin{aligned}
\#\mathcal{A}_{\ell^k,I} &= \#GL_2(\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha])\frac{\#\mathbb{Z}/\ell^k\mathbb{Z}^\times}{\#\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]^{\ \times}} \\
&= \ell^{8k-6}(\ell^4-1)(\ell^2-1)\frac{(\ell-1)\ell^{k-1}}{(\ell^2-1)\ell^{2k-2}} \\
&= \ell^{7k-5}(\ell^4-1)(\ell-1).
\end{aligned}$$

□

Proposition 5.6. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#\mathcal{A}^t_{\ell^k,I} = \frac{(\ell-1)}{(\ell+1)}\ell^{6k-2}\left(\ell^2+\ell+1-\ell^{-2k}\right).$$

Proof. See Appendix A. $\square$

5.2 Split Primes

Let f be as above, suppose that ℓ is an odd split prime in $\mathcal{O}_f$. Then

$$\widehat{\mathcal{O}}_\ell \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

and the morphism induced by the unique non-trivial element of the Galois group of K_f over $\mathbb{Q}$ by the tensor product over $\mathbb{Z}$ with $\mathbb{Z}_\ell$ is

$$\bar{\cdot} : \mathbb{Z}_\ell \times \mathbb{Z}_\ell \to \mathbb{Z}_\ell \times \mathbb{Z}_\ell : (a,b) \mapsto (b,a).$$

In particular the embedding of $\mathbb{Z}$ into $\widehat{\mathcal{O}}_\ell$ is diagonal. Suppose that ℓ has large image in the sense of Theorem 5.2. Then the image of the Galois representation modulo ℓ^k and its subset $\{\sigma \in \mathcal{G}_{\ell^k} \mid \operatorname{tr}\sigma \in \mathbb{Z}/\ell^k\mathbb{Z}\}$ are respectively

$$\begin{aligned}
\mathcal{A}_{\ell^k,S} &:= \{(\tau,\tau') \in GL_2(\mathbb{Z}/\ell^k\mathbb{Z})^2 \mid \det\tau = \det\tau'\} \text{ and}\\
\mathcal{A}^t_{\ell^k,S} &:= \{(\tau,\tau') \in GL_2(\mathbb{Z}/\ell^k\mathbb{Z})^2 \mid \text{char. poly. } \tau = \text{char. poly. } \tau'\},
\end{aligned}$$

where char. poly. $\tau = X^2 - \operatorname{tr}\tau X + \det\tau$ denotes the characteristic polynomial of τ.

Proposition 5.7. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#\mathcal{A}_{\ell^k,S} = \ell^{7k-5}(\ell^2-1)^2(\ell-1).$$

Proof. The determinant is equidistributed in the units of $(\mathbb{Z}/\ell^k\mathbb{Z})^2$. By Corollary 5.4 $\#GL_2(\mathbb{Z}/\ell^k\mathbb{Z})^2 = \left(\ell^{4k-3}(\ell^2-1)(\ell-1)\right)^2$. Moreover there are $\left(\ell^{k-1}(\ell-1)\right)^2$ units in $(\mathbb{Z}/\ell^k\mathbb{Z})^2$ and $\ell^{k-1}(\ell-1)$ are contained in $\mathbb{Z}/\ell^k\mathbb{Z}$. Hence

$$\begin{aligned}
\#\mathcal{A}_{\ell^k,S} &= \#GL_2(\mathbb{Z}/\ell^k\mathbb{Z})^2 \frac{\#\mathbb{Z}/\ell^k\mathbb{Z}^\times}{\#(\mathbb{Z}/\ell^k\mathbb{Z}^\times)^2}\\
&= \left(\ell^{4k-3}(\ell^2-1)(\ell-1)\right)^2 \frac{\ell^{k-1}(\ell-1)}{\left(\ell^{k-1}(\ell-1)\right)^2}\\
&= \ell^{7k-5}(\ell^2-1)^2(\ell-1).
\end{aligned}$$

$\square$

Proposition 5.8. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#\mathcal{A}^t_{\ell^k,S} = \frac{(\ell-1)}{(\ell+1)}\ell^{6k-4}\left(\ell^4+\ell^3-\ell^2-2\ell-\ell^{-2k+2}\right).$$

Proof. See Appendix B. $\square$

5.3 The limit of F_m

In this section we describe the behaviour of the factor F_m and its limit by divisibility.

Lemma 5.9. *Let ℓ be a prime. Then*

$$\widehat{F}_\ell := \lim_{k\to\infty} \ell^k \frac{\#\mathcal{G}^t_{\ell^k}}{\#\mathcal{G}_{\ell^k}} < \infty.$$

Moreover if ℓ is odd, unramified and has large image,

$$\widehat{F}_\ell = \begin{cases} \dfrac{\ell^3(\ell^2+\ell+1)}{(\ell+1)(\ell^4-1)} & \text{if } \ell \text{ is inert} \\ \dfrac{\ell^2(\ell^3+\ell^2-\ell-2)}{(\ell^2-1)^2(\ell+1)} & \text{if } \ell \text{ is split.} \end{cases}$$

Proof. First we show that $\widehat{F}_\ell$ is finite if ℓ is a prime with large image by deducing an upper bound on $\#\mathcal{A}^t_{\ell^k}$ and a lower bound on $\#\mathcal{A}_{\ell^k}$.

Let D be the positive square-free integer such that $K_f = \mathbb{Q}(\sqrt{D})$. Then $\mathcal{O}_f = \mathbb{Z}[X]/(X^2 - D)$ and

$$\mathcal{O}_{\ell^k} \cong (\mathbb{Z}/\ell^k\mathbb{Z}[X])/(X^2 - D).$$

In particular we can embed $\mathcal{A}^t_{\ell^k}$ into

$$M^t_{\ell^k} := \Big\{\sigma \in M_{2\times 2}\big((\mathbb{Z}/\ell^k\mathbb{Z}[X])/(X^2-D)\big) \mid \operatorname{tr}\sigma \in \mathbb{Z}/\ell^k\mathbb{Z} \text{ and } \det\sigma \in \mathbb{Z}/\ell^k\mathbb{Z}\Big\}.$$

We deduce an upper bound on the size of the latter set. Let a_1, a_2, ... and d_2 be elements of $\mathbb{Z}/\ell^k\mathbb{Z}$ and $\sigma = \begin{pmatrix} a_1 + Xa_2 & b_1 + Xb_2 \\ c_1 + Xc_2 & d_1 + Xd_2 \end{pmatrix}$ then

$$\begin{aligned} \operatorname{tr}\sigma \in \mathbb{Z}/\ell^k\mathbb{Z} &\Leftrightarrow a_2 + d_2 = 0 \text{ and} \\ \det\sigma \in \mathbb{Z}/\ell^k\mathbb{Z} &\Leftrightarrow a_1d_2 + a_2d_1 - b_1c_2 - b_2c_1 = 0. \end{aligned}$$

In particular there is a bijection of sets between $M^t_{\ell^k}$ and the 7-tuples $(a_1, a_2, ..., d_1)$ satisfying

$$a_1a_2 - a_2d_1 + b_1c_2 + b_2c_1 = 0. \tag{1}$$

Denote by υ the ℓ-adic valuation on $\mathbb{Z}/\ell^k\mathbb{Z}$. Let $t = \min\{k, \upsilon(a_2), \upsilon(b_2), \upsilon(c_2)\}$. If $t = k$, then (1) holds for any a_1, b_1, c_1 and d_1 in $\mathbb{Z}/\ell^k\mathbb{Z}$. So there are at most ℓ^{4k} matrices in $M^t_{\ell^k}$ with $a_2 = b_2 = c_2 = 0$.

Suppose that t is strictly smaller than k. Take a'_2, b'_2 and c'_2 such that $a_2\ell^t = a'_2\ell^t$, $b_2 = b'_2\ell^t$ and $c_2 = c'_2\ell^t$. By construction at least one of a'_2, b'_2 or c'_2 is invertible in $\mathbb{Z}/\ell^{k-t}\mathbb{Z}$. Suppose that a'_2 is a unit. Then

$$(1) \Leftrightarrow d_1 \equiv a'^{-1}_2\big(a_1a'_2 + b_1c'_2 + b'_2c_1\big) \mod \ell^{k-t}.$$

Hence for every $0 \le t < k$ there are at most $\ell^{6k-2t-1}(\ell-1)$ matrices in $M^t_{\ell^k}$ with $\upsilon(a_2)=t$, $\upsilon(b_2)\ge t$ and $\upsilon(c_2)\ge t$. If b'_2 or c'_2 is invertible we obtain at most $\ell^{6k-2t-1}(\ell-1)$ matrices in $M^t_{\ell^k}$ by a similar argument. So for every $t<k$ there are at most $3\ell^{6k-2t-1}(\ell-1)$ matrices in $M^t_{\ell^k}$ with $t=\min\{\upsilon(a_2),\upsilon(b_2),\upsilon(c_2)\}$. Summing over all t yields

$$\begin{aligned}
\#\mathcal{A}^t_{\ell^k} \le \#M^t_{\ell^k} &\le \ell^{4k} + 3\sum_{t=0}^{k-1} \ell^{6k-2t-1}(\ell-1)\\
&= \ell^{4k} + 3(\ell-1)\ell^{4k-1}\big(\ell^{2k}+\ell^{2k-2}+\cdots+\ell^2\big)\\
&= \ell^{4k}\left(1+3(\ell-1)\ell\frac{(\ell^{2k}-1)}{(\ell^2-1)}\right)\\
&\le 3\ell^{6k}.
\end{aligned}$$

Next we deduce a lower bound on $\#\mathcal{A}_{\ell^k}$. Let u and v be units in $\mathbb{Z}/\ell^k\mathbb{Z}$,$b$ and c elements of $(\mathbb{Z}/\ell^k\mathbb{Z}[X])/(X^2-D)$ and $m \in \ell\mathbb{Z}/\ell^k\mathbb{Z}$. Then $a=(v+mX)$ is a unit in $(\mathbb{Z}/\ell^k\mathbb{Z}[X])/(X^2-D)$. Indeed the inverse is given by $(v^2-m^2D)^{-1}(v-mX)$. If $d=(u+bc)a^{-1}$ the matrix $\sigma = \begin{pmatrix} a & b\\ c & d\end{pmatrix}$ has determinant u so belongs to $\mathcal{A}_{\ell^k}$. In particular there are at least $\ell^{7k-3}(\ell-1)^2$ elements in $\mathcal{A}_{\ell^k}$. Using the upper bound on $\#\mathcal{A}^t_{\ell^k}$ and the lower bound on $\#\mathcal{A}_{\ell^k}$ we obtain

$$\widehat{F}_\ell = \lim_{k\to\infty} \ell^k \frac{\#\mathcal{A}^t_{\ell^k}}{\#\mathcal{A}_{\ell^k}} \le \lim_{k\to\infty} \ell^k \frac{3\ell^{6k+1}}{\ell^{7k-3}(\ell^2-1)} \le 4\ell^2.$$

If ℓ is an exceptional prime, then $\widehat{\mathcal{G}}_\ell$ is an open subgroup of $\widehat{\mathcal{A}}_\ell$ by Theorem 5.2. So that

$$\lim_{k\to\infty} \frac{\#\mathcal{A}_{\ell^k}}{\#\mathcal{G}_{\ell^k}} = \#\left(\widehat{\mathcal{A}}_\ell/\widehat{\mathcal{G}}_\ell\right) < \infty.$$

Moreover, $\mathcal{G}^t_{\ell^k} \subset \mathcal{A}^t_{\ell^k}$ so

$$\begin{aligned}
\widehat{F}_\ell = \lim_{k\to\infty} \ell^k \frac{\#\mathcal{G}^t_{\ell^k}}{\#\mathcal{G}_{\ell^k}} &\le \lim_{k\to\infty} \ell^k \frac{\#\mathcal{A}^t_{\ell^k}}{\#\mathcal{G}_{\ell^k}}\\
&= \lim_{k\to\infty} \ell^k \frac{\#\mathcal{A}^t_{\ell^k}}{\#\mathcal{A}_{\ell^k}} \cdot \lim_{k\to\infty} \frac{\#\mathcal{A}_{\ell^k}}{\#\mathcal{G}_{\ell^k}}\\
&< \infty.
\end{aligned}$$

Finally from Propositions 5.5 and 5.7 we obtain

$$\#\mathcal{A}_{\ell^k} = \begin{cases} \ell^{7k-5}(\ell^4-1)(\ell-1) & \text{if } \ell \text{ is inert}\\ \ell^{7k-5}(\ell^2-1)^2(\ell-1) & \text{if } \ell \text{ is split.}\end{cases}$$

Moreover from Propositions 5.6 and 5.8

$$\#\mathcal{A}^t_{\ell^k} = \begin{cases} \frac{\ell-1}{\ell+1}\ell^{6k-2}\left(\ell^2+\ell+1-\ell^{-2k}\right) & \text{if } \ell \text{ is inert} \\ \frac{\ell-1}{\ell+1}\ell^{6k-4}\left(\ell^4+\ell^3-\ell^2-2\ell-\ell^{-2k+2}\right) & \text{if } \ell \text{ is split.} \end{cases}$$

So that

$$\lim_{k\to\infty} \ell^k \frac{\#\mathcal{A}^t_{\ell^k}}{\#\mathcal{A}_{\ell^k}} = \begin{cases} \dfrac{\ell^3(\ell^2+\ell+1)}{(\ell+1)(\ell^4-1)} & \text{if } \ell \text{ is inert} \\ \dfrac{\ell^2(\ell^3+\ell^2-\ell-2)}{(\ell^2-1)^2(\ell+1)} & \text{if } \ell \text{ is split.} \end{cases}$$

□

Corollary 5.10. *Let f be as above. Then the limit of F_m by divisibility exists, i.e.,*

$$\widehat{F} := \lim_{m\to|\infty} F_m < \infty.$$

Proof. First note that for any sequence a_n

$$\sum_n a_n < \infty \Rightarrow \sum_n \log(a_n+1) < \infty$$
$$\Leftrightarrow \prod_n (a_n+1) < \infty.$$

Moreover if ℓ is an odd unramified prime with large image, Lemma 5.9 yields

$$\widehat{F}_\ell = \begin{cases} 1 + \dfrac{\ell^3+\ell+1}{(\ell+1)(\ell^4-1)} & \text{if } \ell \text{ is inert} \\ 1 + \dfrac{\ell^3-\ell-1}{(\ell^2-1)^2(\ell+1)} & \text{if } \ell \text{ is split.} \end{cases}$$

In particular the product $\prod \widehat{F}_\ell$ taken over all odd unramified primes with large image is finite. Since almost all primes are odd, are unramified and have large image the product taken over all primes is finite by Lemma 5.9. Finally Serre's adelic open image theorem [11,

Theorem 3.3.1] states that $\widehat{\mathcal{G}}$ is an open subgroup of $\prod_\ell \widehat{\mathcal{G}}_\ell$ hence

$$\begin{aligned}
\lim_{m\to|\infty} F_m &= \lim_{m\to|\infty} m\frac{\#\mathcal{G}_m^t}{\#\mathcal{G}_m} \\
&\leq \lim_{m\to|\infty} \frac{\prod_{\ell^k\|m} \ell^k \#\mathcal{G}_{\ell^k}^t}{\#\mathcal{G}_m} \\
&= \lim_{m\to|\infty} \frac{\prod_{\ell^k\|m} \ell^k \#\mathcal{G}_{\ell^k}^t}{\prod_{\ell^k\|m} \#\mathcal{G}_{\ell^k}} \cdot \frac{\prod_{\ell^k\|m} \#\mathcal{G}_{\ell^k}}{\#\mathcal{G}_m} \\
&= \lim_{m\to|\infty} \prod_{\ell^k\|m} \ell^k \frac{\#\mathcal{G}_{\ell^k}^t}{\#\mathcal{G}_{\ell^k}} \cdot \lim_{m\to|\infty} \frac{\# \prod_{\ell^k\|m} \mathcal{G}_{\ell^k}}{\#\mathcal{G}_m} \\
&= \prod_\ell \widehat{F}_\ell \cdot \# \left(\prod_\ell \widehat{\mathcal{G}}_\ell / \widehat{\mathcal{G}} \right) \\
&< \infty.
\end{aligned}$$

□

6 Main Result

In this section we state and prove our main result.

Lemma 6.1. *Let f be a weight 2 normalized cuspidal Hecke eigenform of level $\Gamma_1(N)$, with quadratic coefficient field without inner twist. Let m be a positive integer such that Assumptions 4.4 and 3.2 hold. Then*

$$\#\{p < x \text{ prime} \mid a_p \in \mathbb{Q}\} \sim \frac{F_m}{\alpha_m} \frac{16\sqrt{D}}{3\pi^2} \frac{\sqrt{x}}{\log x},$$

with $0 < \alpha_m < \infty$ as in Assumption 3.2.

Proof. Denote $N_f(x) = \#\{p < x \text{ prime } \mid a_p(f) \in \mathbb{Q}\} = P(x) \cdot \pi(x)$ and let $\varepsilon > 0$. By Assumption 3.2 there exists $x_1 > 0$ such that for all $x > x_1$

$$\left| \frac{P^m(x) P_m(x)}{\alpha_m P(x)} - 1 \right| < \varepsilon/6.$$

Let x_2 be such that for all $x > x_2$ we have

$$\left| \frac{F_m}{m P_m(x)} - 1 \right| < \frac{\varepsilon}{6}.$$

Such an x_2 exists by Lemma 5.1. By Corollary 4.6 under Assumption 4.4 there exists an x_3 such that for all $x > x_3$

$$\left| \frac{16 m \sqrt{D}}{3\pi^2 \sqrt{x} P^m(x)} - 1 \right| < \frac{\varepsilon}{6}.$$

Finally let x_4 be such that for all $x > x_4$

$$\left|\frac{x}{\pi(x)\log(x)} - 1\right| < \frac{\varepsilon}{6}.$$

Then for any $x > \max\{x_1, x_2, x_3, x_4\}$ we obtain

$$\begin{aligned}\left|\frac{1}{\alpha_m}\frac{16\sqrt{D}F_m\sqrt{x}}{3\pi^2\log x N_f(x)} - 1\right| &= \left|\frac{P^m(x)P_m(x)}{\alpha_m P(x)}\cdot\frac{16\sqrt{D}m}{3\pi^2\sqrt{x}P^m(x)}\cdot\frac{F_m}{mP_m(x)}\cdot\frac{x}{\pi(x)\log x} - 1\right| \\ &< \left|\left(1+\frac{\varepsilon}{6}\right)^4 - 1\right| \\ &< \varepsilon.\end{aligned}$$

□

Corollary 6.2. *Let f be as above. Suppose that there exists a positive integer m_0 such that Assumptions 4.4 and 3.2 hold for m_0.*

1. *Then Assumption 4.4 implies 3.2 for any positive integer m.*
2. *If Assumption 4.4 is true for all positive integers $m \in M\mathbb{Z}$ for some M, then*

$$0 < \lim_{m\to|\infty}\lim_{x\to\infty}\frac{P^m(x)\cdot P_m(x)}{P(x)} =: \alpha < \infty.$$

   Moreover

$$\#\{p < x \text{ prime } \mid a_p(f) \in \mathbb{Q}\} \sim \frac{\widehat{F}}{\alpha}\frac{16\sqrt{D}}{3\pi^2}\frac{\sqrt{x}}{\log x}.$$

Proof. If such an m_0 exists then by Lemma 6.1 there exists a positive non-zero constant C_{m_0} such that $P(x) \sim C_{m_0}\sqrt{x}/\log x$.

1. Let m be a positive integer satisfying Assumption 4.4. By Corollary 4.6 and Lemma 5.1 $P^m(x)\cdot P_m(x) \sim C'\sqrt{x}/\log x$ with $0 < C' = \frac{16\sqrt{D}F_m}{3\pi^2} < \infty$. Hence

$$\begin{aligned}\lim_{x\to\infty}\frac{P^m(x)\cdot P_m(x)}{P(x)} &= \lim_{x\to\infty}\frac{C'\sqrt{x}/\log x}{C_{m_0}\sqrt{x}/\log x} \\ &= \frac{C'}{C_{m_0}}.\end{aligned}$$

2. By the first point we can apply Lemma 6.1 to any pair of positive integers m and m' in $M\mathbb{Z}$ and obtain that

$$\frac{\alpha_m}{F_m} = \frac{\alpha_{m'}}{F_{m'}}.$$

So the following definition of α does not depend on the choice of m.

$$0 < \alpha := \frac{\alpha_m \widehat{F}}{F_m} < \infty.$$

In particular

$$\begin{aligned}\lim_{m \to | \infty} \lim_{x \to \infty} \frac{P^m(x) \cdot P_m(x)}{P(x)} &= \lim_{m \to | \infty} \alpha_m \\ &= \lim_{m \to | \infty} \frac{\alpha F_m}{\widehat{F}} \\ &= \alpha.\end{aligned}$$

By Lemma 6.1 we obtain for every positive integer m divisible by M that

$$1 = \lim_{x \to \infty} \frac{F_m 16 \sqrt{D} \sqrt{x}}{\alpha_m 3\pi^2 \log x N_f(x)}.$$

Taking the limit by divisibility of m yields

$$1 = \lim_{m \to | \infty} \lim_{x \to \infty} \frac{F_m 16 \sqrt{D} \sqrt{x}}{\alpha_m 3\pi^2 \log x N_f(x)}.$$

Since F_m and α_m do not depend on x we obtain

$$\begin{aligned}1 &= \lim_{m \to | \infty} \frac{F_m}{\alpha_m} \lim_{x \to \infty} \frac{16 \sqrt{D} \sqrt{x}}{3\pi^2 \log x N_f(x)} \\ &= \lim_{x \to \infty} \frac{\widehat{F} 16 \sqrt{D} \sqrt{x}}{\alpha 3\pi^2 \log x N_f(x)}.\end{aligned}$$

□

Theorem 6.3. *Let f be a weight 2 normalized cuspidal Hecke eigenform of level $\Gamma_1(N)$ with quadratic coefficient field $\mathbb{Q}(\sqrt{D})$ and without inner twist. Suppose that there exists a positive integer m_0 such that Assumptions 4.4 and 3.1 hold for f and all positive integers in $m_0\mathbb{Z}$. Then*

$$\#\{p < x \text{ prime } \mid a_p(f) \in \mathbb{Q}\} \sim \frac{16\sqrt{D}\widehat{F}}{3\pi^2} \frac{\sqrt{x}}{\log x}.$$

Proof. From Corollary 6.2 we obtain

$$\#\{p < x \text{ prime } \mid a_p(f) \in \mathbb{Q}\} \sim \frac{\widehat{F}}{\alpha} \frac{16\sqrt{D}}{3\pi^2} \frac{\sqrt{x}}{\log x}.$$

The claim of Assumption 3.1 is precisely that $\alpha = 1$. Hence the theorem follows. □

7 Numerical Results

In this section we provide numerical results that support the assumptions made and the results deduced from these assumptions. Moreover we describe the method used to obtain these results.

All computations are done using the following six new Hecke eigenforms $f_N \in S_2(\Gamma_0(N))$:

$$\begin{aligned}
f_{29} &= q + (-1+\sqrt{2})q^2 + (1-\sqrt{2})q^3 + (1-2\sqrt{2})q^4 - q^5 + \cdots \\
f_{43} &= q + \sqrt{2}q^2 - \sqrt{2}q^3 + (2-\sqrt{2})q^5 + \cdots \\
f_{55} &= q + (1+\sqrt{2})q^2 - 2\sqrt{2}q^3 + (1+2\sqrt{2})q^4 - q^5 \cdots \\
f_{23} &= q + \frac{-1+\sqrt{5}}{2}q^2 - \sqrt{5}q^3 - \frac{1+\sqrt{5}}{2}q^4 + (-1+\sqrt{5})q^5 + \cdots \\
f_{87} &= q + \frac{1+\sqrt{5}}{2}q^2 + q^3 + \frac{-1+\sqrt{5}}{2}q^4 + (1-\sqrt{5})q^5 \cdots \\
f_{167} &= q + \frac{-1+\sqrt{5}}{2}q^2 - \frac{1+\sqrt{5}}{2}q^3 - \frac{1+\sqrt{5}}{2}q^4 - q^5 + \cdots .
\end{aligned}$$

Note that the level for each of the eigenforms is square-free and the nebentypus is trivial so by Lemma 2.1 none of these eigenforms have inner twists. Moreover the coefficient field of f_{29}, f_{43} and f_{55} is $\mathbb{Q}(\sqrt{2})$ and the coefficient field of f_{23}, f_{87} and f_{167} is $\mathbb{Q}(\sqrt{5})$. In this section we will denote $\mathcal{A}_{f_N}$, c_{f_N},... by $\mathcal{A}_N$, c_N, ... respectively.

As described in Section 4 the Galois orbit of the p-th coefficient of a eigenform f_N can be computed from the L_p-polynomial of the abelian variety $\mathcal{A}_N$ associated to f_N. For each eigenform f_N we give an equation for a hyperelliptic curve C_N such that the Jacobian $J(C_N)$ is isomorphic to the abelian variety $\mathcal{A}_N$. Obtaining such an equation is a non-trivial problem. For levels 29, 43 and 55 the equations are found in [1, page 42] and [18, page 137] for the remaining three. The equations are:

$$\begin{aligned}
C_{29} &: y^2 = x^6 - 2x^5 + 7x^4 - 6x^3 + 13x^2 - 4x + 8, \\
C_{43} &: y^2 = -3x^6 - 2x^5 + 7x^4 - 4x^3 - 13x^2 + 10x - 7, \\
C_{55} &: y^2 = -3x^6 + 4x^5 + 16x^4 - 2x^3 - 4x^2 + 4x - 3, \\
C_{23} &: y^2 = x^6 + 2x^5 - 23x^4 + 50x^3 - 58x^2 + 32x - 11, \\
C_{87} &: y^2 = -x^6 + 2x^4 + 6x^3 + 11x^2 + 6x + 3, \\
C_{167} &: y^2 = -x^6 + 2x^5 + 3x^4 - 14x^3 + 22x^2 - 16x + 7.
\end{aligned}$$

Next we use Andrew Sutherlands smalljac algorithm described in [7] to compute the coefficients of the L_p-polynomial of each hyperelliptic curve C_N. This algorithm is implemented in C and is available at Sutherland's web page. With this method we are able to compute the Galois orbit of the coefficients of one eigenform for all primes up to 10^8 in less than 50 hours. All computations are done on a Dell Latitude E6540 laptop with Intel i7-4610M processor (3.0 GHz, 4MB cache, Dual Core). The processing of the data and the creation

of the graphs was done using Sage Mathematics Software [17] on the same machine. The running time of this is negligible compared to the smalljac algorithm.

7.1 Murty's Conjecture

First we check Conjecture 1.1. For each eigenform we plot the number of primes $p < x$ such that the p-th coefficient is a rational integer for 50 values of x up to 10^8. According to this conjecture there exists a constant c_N such that

$$\#\{p < x \text{ prime} \mid a_p(f_N) \in \mathbb{Q}\} \sim c_N \frac{\sqrt{x}}{\log x}.$$

To check the conjecture we approximate c_N using least squares fitting. Denote this estimate by $\widetilde{c}_N$. Figure 2 provides numerical evidence for the behaviour of $N(x)$ and column 2 of Table 1 list the values of $\widetilde{c}_N$ found by least squares fitting.

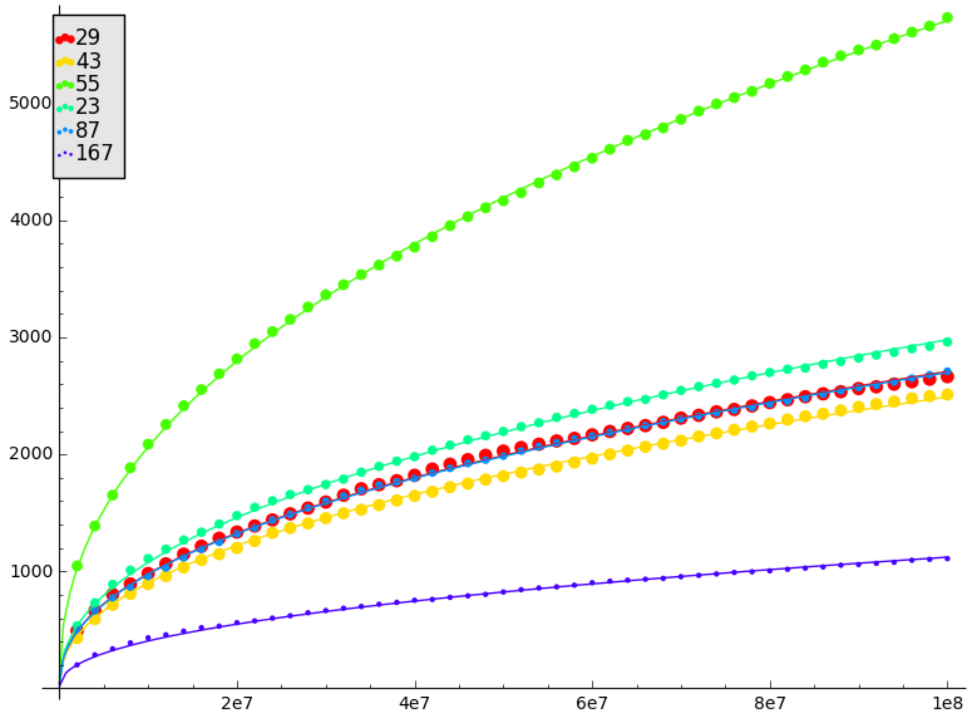


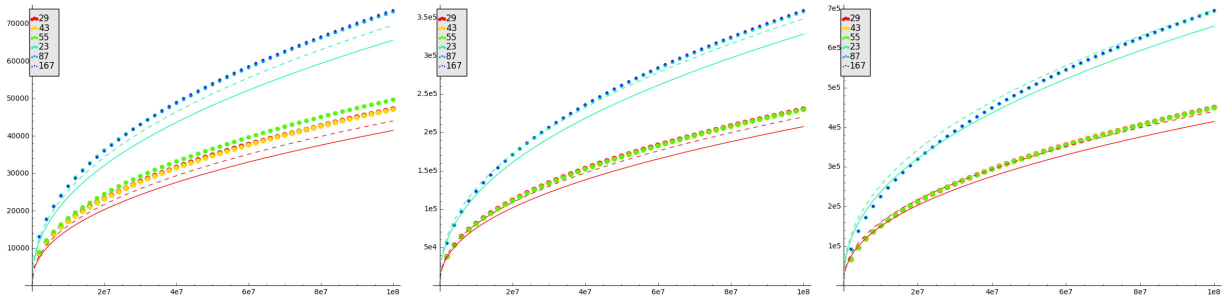
Figure 2: Plot of $\#\{p < x \text{ prime} \mid a_p(f_N) \in \mathbb{Q}\}$ (dots) and $\widetilde{c}_N\sqrt{x}/\log x$ (line) using least squares fitting to compute $\widetilde{c}_N$ for x up to 10^8.

7.2 The place at infinity

Corollary 4.6 states that under Assumption 4.4 and the generalized Sato-Tate conjecture

$$\#\left\{p < x \text{ prime} \mid Z_p \in]-m\sqrt{D}/2, m\sqrt{D}/2[\right\} \sim \frac{16\sqrt{D}m}{3\pi^2}\frac{\pi(x)}{\sqrt{x}}.$$

For m equal to 100, 500 and 1000 Figure 3 indicates that $\frac{16m\sqrt{D}}{3\pi^2}\frac{\pi(x)}{\sqrt{x}}$ is in fact a good approximation for $\#\{p < x \text{ prime} \mid Z_p \in]-m\sqrt{D}/2, m\sqrt{D}/2[\}$. Although this neither proves Assumption 4.4 nor the generalized Sato-Tate conjecture, it does confirm that $P_m(x)$ depends on the coefficient field of the eigenform.



(a) $m = 100$ (b) $m = 500$ (c) $m = 1000$

Figure 3: Plots of $\#\{p < x \text{ prime} \mid Z_p \in]-m\sqrt{D}/2, m\sqrt{D}/2[\}$ (dots), $\frac{16\sqrt{D}m}{3\pi^2}\frac{\pi(x)}{\sqrt{x}}$ (dashed) and $\frac{16\sqrt{D}m}{3\pi^2}\frac{\sqrt{x}}{\log x}$ (full line) for $\sqrt{D} = \sqrt{5}$ (cyan) and $\sqrt{D} = \sqrt{2}$ (red) for each eigenform f_N and $m = 100$, 500, 1000.

7.3 Finite Places

In [2] Nicolas Billerey and Luis Dieulefait provide explicit bounds on the primes ℓ that do not have large image for a given eigenform $f \in S_2(\Gamma_0(N))$ with square-free level N. In fact they provide a more general result. We only state the lemma for square-free level.

Lemma 7.1. *Let f be a eigenform in $S_2(\Gamma_0(N))$. Assume that $N = p_1p_2\cdots p_t$, where $p_1, ..., p_t$ are $t \geq 1$ distinct primes and ℓ is exceptional. Then ℓ divides $15N$ or $p_i^2 - 1$ for some $1 \leq i \leq t$.*

Proof. This is the statement of [2, Theorem 2.6] in the weight 2 case. □

The eigenforms in our computations have weight 2 and square-free level so we can apply the lemma and obtain a list of primes that are possibly exceptional for each eigenform (Table 1).

If ℓ is an odd unramified prime with large image Lemmas 5.1 and 5.9 yield

$$\#\{p < x \text{ prime} \mid Z_p \equiv 0 \mod \ell^k\} \sim \pi(x) \cdot \begin{cases} \dfrac{\ell^2 + \ell + 1 - \ell^{-2k}}{(\ell+1)(\ell^4 - 1)\ell^{k-3}} & \text{if } \ell \text{ is inert} \\ \dfrac{\ell^4 + \ell^3 - \ell^2 - 2\ell - \ell^{-2k+2}}{(\ell^2 - 1)^2 \ell^{k-1}} & \text{if } \ell \text{ is split.} \end{cases}$$

For each prime that is possibly exceptional and each eigenform we can confirm that the prime is exceptional by comparing $\#\{p < x \text{ prime} \mid Z_p \equiv 0 \mod \ell^k\}$ with the expected value for a prime with large image for x up to 10^8 (Fig. 4). For $\ell = 2$ we do not have a theoretic result for large image. Therefore none is plotted. The same holds for $\ell = 5$ and eigenforms f_{23}, f_{87} and f_{167} since 5 ramifies in $\mathbb{Q}(\sqrt{5})$.

Some primes are inert in $\mathbb{Q}(\sqrt{5})$ and split in $\mathbb{Q}(\sqrt{2})$ or vice versa. So a priori we have two possibilities for the behaviour of $\#\{p < x \text{ prime} \mid Z_p \equiv 0 \mod \ell^k\}$ for a prime ℓ with large image. However the first prime for which this occurs is 7. Indeed 7 splits in $\mathbb{Q}(\sqrt{2})$ and is inert in $\mathbb{Q}(\sqrt{5})$. For $\ell = 7$ one can hardly distinguish the inert and split case visually.

From Figure 4 we can confirm that an odd unramified prime is exceptional for a given eigenform if the plot of $\#\{p < x \mid Z_p \equiv 0 \mod \ell^k\}$ differs from that of the large image case. Moreover for any prime ℓ we can conclude that the image of the ℓ-adic representation attached to different eigenforms is distinct. Note that the converse does not hold. Indeed the fact that two eigenforms exhibit the same behaviour with respect to $\#\{p < x \text{ prime} \mid Z_p \equiv 0 \mod \ell^k\}$ does not imply that their ℓ-adic representations are the same.

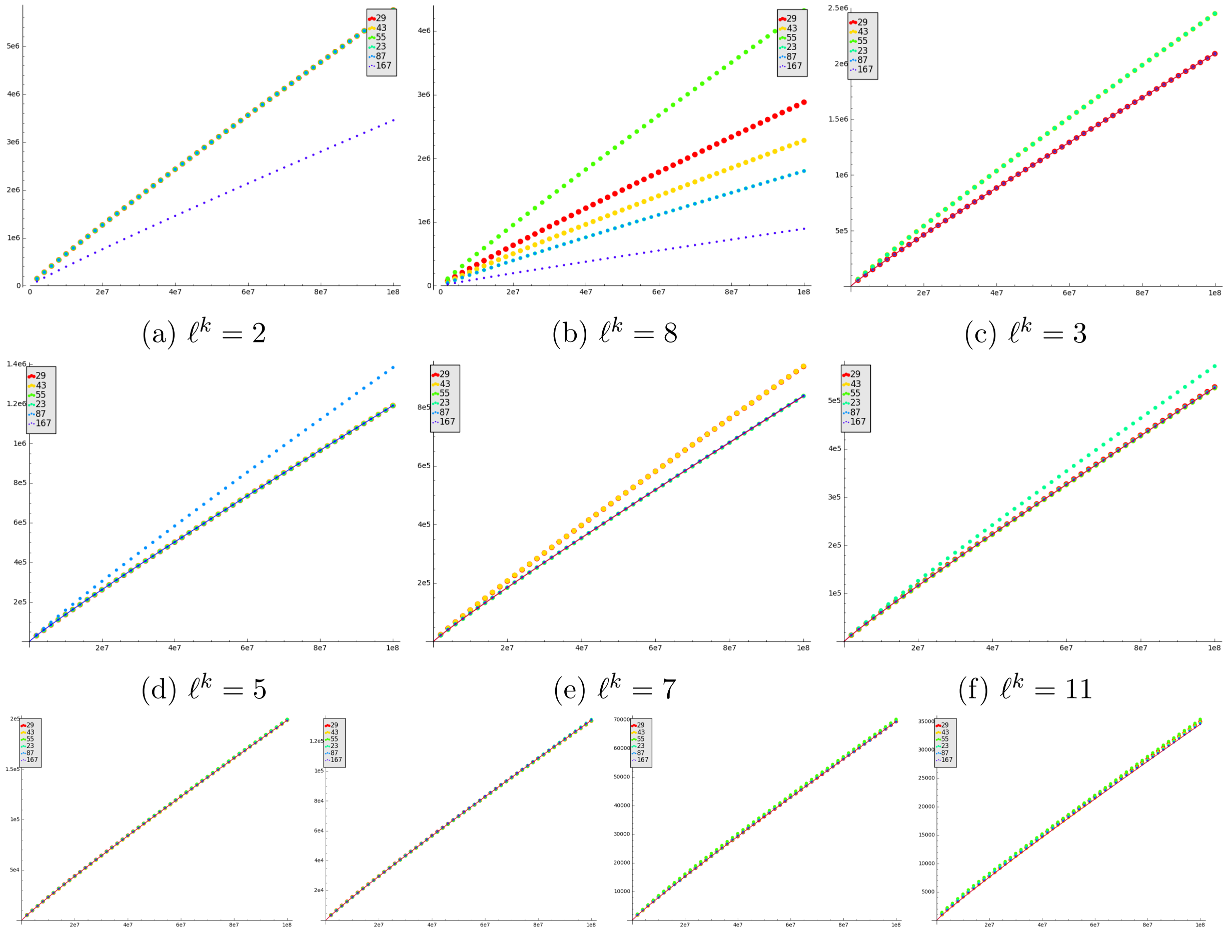
For example if $\ell^k = 2$ (Fig. 4a), then all eigenforms except f_{167} exhibit the same behaviour. But for $\ell^k = 8$ (Fig. 4b) we clearly distinguish five different representations. Note that we do not observe this behaviour for any other prime. From $\ell^k = 3$ (Fig. 4c) we can conclude that 3 is an exceptional prime for the 3-adic representation attached to f_{43} and f_{55}. The primes that are marked in bold in the last column of Table 1 are the primes for which Figure 4 confirms the prime is exceptional.

7.4 Main Result

Next we test Theorem 6.3 by comparing the behaviour of $\#\{p < x \text{ prime} \mid a_p \in \mathbb{Q}\}$ with $c_N\sqrt{x}/\log x$ where c_N is the constant predicted by Theorem 6.3. Recall that according to our main theorem under Assumptions 4.4 and 3.1 and the generalized Sato-Tate conjecture

$$c_N = \frac{16\sqrt{D}}{3\pi^2}\widehat{F}.$$

Since $\widehat{F}$ is a limit by divisibility we approximate it numerically. In order to do so we use the following assumption.



(a) $\ell^k = 2$ (b) $\ell^k = 8$ (c) $\ell^k = 3$

(d) $\ell^k = 5$ (e) $\ell^k = 7$ (f) $\ell^k = 11$

(g) $\ell^k = 29$ (h) $\ell^k = 43$ (i) $\ell^k = 83$ (j) $\ell^k = 167$

Figure 4: Plots of $\#\{p < x \text{ prime} \mid Z_p \equiv 0 \mod \ell^k\}$ for large image (line) and actual value (dots) for all eigenforms. If $\ell = 2$ no function is plotted for large image.

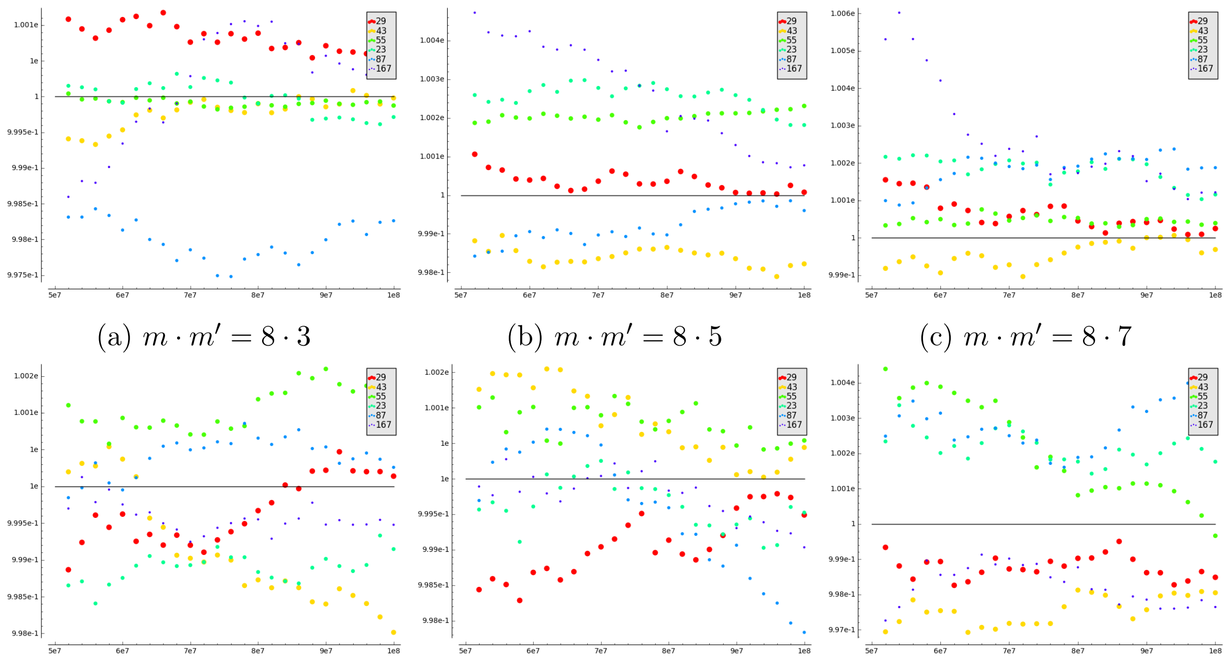
Assumption 7.2. *Let m and m' be co-prime integers. Then*

$$P_m(x) \cdot P_{m'}(x) \sim P_{m \cdot m'}(x).$$

If $\widehat{\rho}$ is an independent system of representations in the sense of [16, Section 3], the assumption holds. However $\widehat{\rho}$ is in general not an independent system and the assumption is a much weaker claim. Moreover this assumption is only needed to get a numerical result and our main theorem holds even if this assumption is false. All computations support the assumption.

Under Assumption 7.2 we can compute an approximation of $\widehat{F}$ by taking the product over all primes

$$\widehat{F} = \prod_{\ell} \widehat{F}_\ell.$$



(a) $m \cdot m' = 8 \cdot 3$ (b) $m \cdot m' = 8 \cdot 5$ (c) $m \cdot m' = 8 \cdot 7$

(d) $m \cdot m' = 3 \cdot 5$ (e) $m \cdot m' = 3 \cdot 7$ (f) $m \cdot m' = 5 \cdot 7$

Figure 5: Plots of $P_m(x) \cdot P_{m'}(x)/P_{m \cdot m'}(x)$.

For odd unramified primes with large image the factor $\widehat{F}_\ell$ is given by Lemma 5.9. Let $\{\ell_1, ..., \ell_t\}$ be the set of primes that are even, ramified or possibly exceptional. For every prime ℓ_i we apply Lemma 5.1 for $\ell_i^{k_i}$ with k_i the largest integer such that $\ell_i^{k_i}$ is less than $\sqrt{10^8}/20$, i.e.,

$$k_i = \lfloor \log_{\ell_i}(\sqrt{10^8}/20) \rfloor.$$

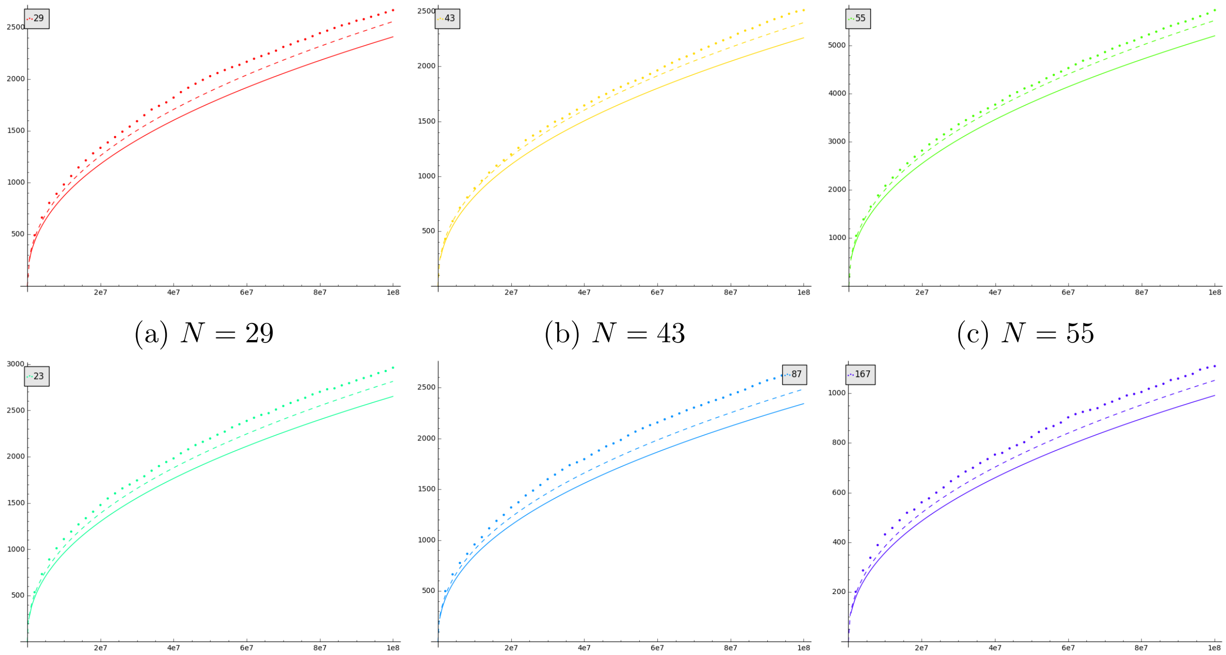
So we use the following approximation for c_N

$$\widehat{c}_N = \frac{16\sqrt{D}}{3\pi^2} \prod_{i=1}^{t} \ell^{k_i} P_{\ell_i^{k_i}}(10^8) \prod_{\substack{\ell \text{ unramified} \\ \text{with large image}}} \widehat{F}_\ell.$$

For every eigenform f_N we plot $\widehat{c}_N \sqrt{c}/\log x$, $\widehat{c}_N \pi(x)/\sqrt{x}$ and $\#\{p < x \text{ prime} \mid a_p \in \mathbb{Q}\}$ (see figure 6).

Comparing the values of $\widehat{c}_N$ to the previously found $\widetilde{c}_N$ by least square fitting yields $1.025 < \widetilde{c}_N/\widehat{c}_N < 1.149$ (Table 1). This error is to be expected for this small a bound on the primes. For example in the proof of Corollary 4.6 we use $\frac{\sqrt{x}}{\log x}$ to approximate $\sum_{p=2}^{x} \frac{1}{2\sqrt{p}}$. For $x = 10^8$ this estimate yields a similar error

$$\frac{\log 10^8}{\sqrt{10^8}} \cdot \sum_{p=2}^{10^8} \frac{1}{2\sqrt{p}} = 1.146 \cdots .$$



(a) $N = 29$ (b) $N = 43$ (c) $N = 55$

(d) $N = 23$ (e) $N = 87$ (f) $N = 167$

Figure 6: Plots of $\#\{p < x \text{ prime} \mid a_p \in \mathbb{Q}\}$ (dots), $\widehat{c}_N \frac{\sqrt{x}}{\log x}$ (full line) and $\widehat{c}_N \frac{\pi(x)}{\sqrt{x}}$ (dashed line) for all eigenforms f_N with $\widehat{c}_N$ based on Theorem 6.3 .

7.5 Final Assumption

The final assumptions we check are Assumptions 3.1 and 3.2. Recall that Assumption 3.1 states that for every eigenform f_N and every $\varepsilon > 0$ there exists an m_0 such that for all m with $m_0|m$ there exists an x_0 such that for all $x > x_0$

$$\left| \frac{P^m(x) \cdot P_m(x)}{P(x)} - 1 \right| < \varepsilon.$$

Assumption 3.2 is a much weaker claim and states that the limit

$$\lim_{x \to \infty} \frac{P^m(x) \cdot P_m(x)}{P(x)}$$

exists for a given positive m. For all eigenforms we can find various m such that

$$\left| \frac{P^m(x) \cdot P_m(x)}{P(x)} - 1 \right| < 0.2$$

for all x larger than $5 \cdot 10^7$. For every eigenform we choose different values for m and plot $\frac{P^m(x) \cdot P_m(x)}{P(x)}$ and the constant functions 1 and $\frac{P^{m_N}(10^8) \cdot P_{m_N}(10^8)}{P(10^8)}$ (Fig. 7). Where m_N is the

Table 1: For each eigenform f_N the table contains the level N, the constant $\widetilde{c}_N$ obtained by least square fitting, the constant $\widehat{c}_N$ according to Theorem 6.3, the error $\widetilde{c}_N/\widehat{c}_N$ and the possibly exceptional primes according to Corollary 7.1 respectively. The confirmed exceptional primes are marked in bold.

N	$\widetilde{c}_N$	$\widehat{c}_N$	$\widetilde{c}_N/\widehat{c}_N$	Pos. exc. primes
29	4.990	4.517	1.104	2, 3, 5, **7**, 29
43	4.588	4.204	1.109	2, **3**, 5, **7**, 11, 43
55	10.515	9.958	1.056	2, **3**, 5 ,11
23	5.490	4.982	1.102	2, 3, 5, **11**, 23
87	4.972	4.413	1.127	2, 3, **5**, 7, 29
167	2.066	1.833	1.127	2, 3, 5, 7, 83, 167

largest positive integer used for every eigenform f_N. The values of m are chosen so that they increase by divisibility and so that the confirmed exceptional primes divide m.

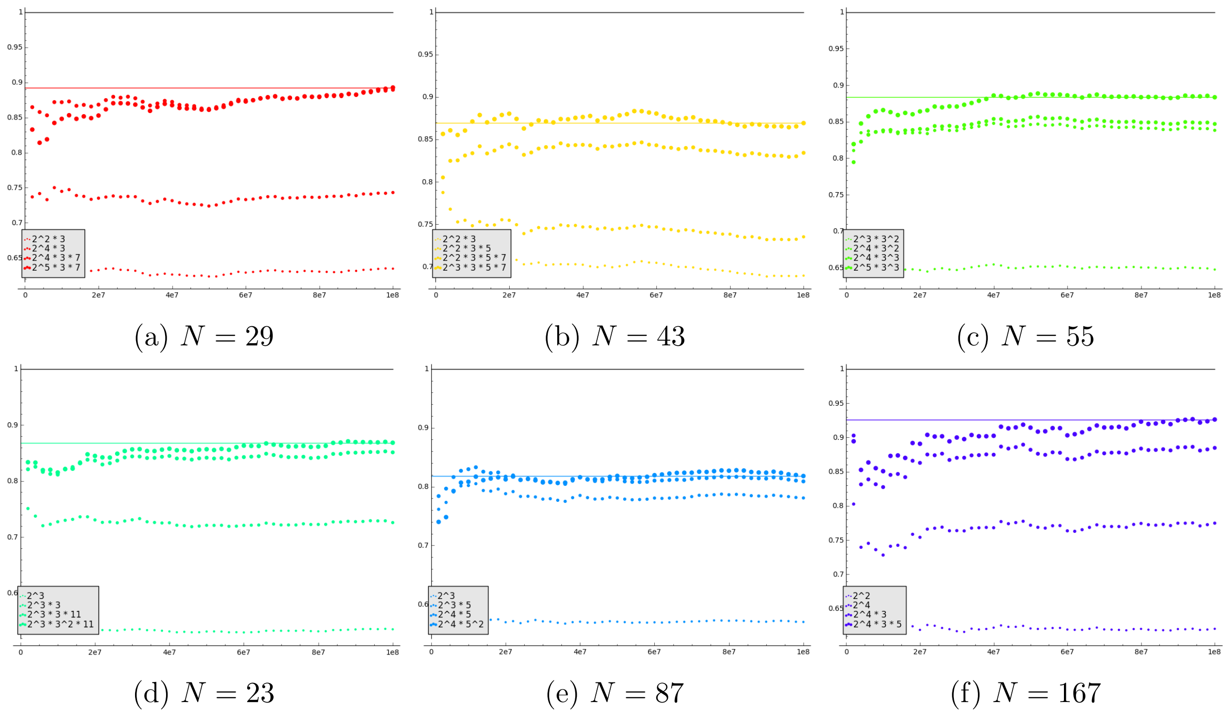
Additionally figure 7 provides numerical evidence for Assumption 3.2 which implies the existence of the double limit of $P_m(x) \cdot P^m(x)/P(x)$ by Corollary 6.2. However one could argue that the figure suggests that the double limit does not converge to 1. Let us denote for every N

$$\alpha_N = \lim_{m \to | \infty} \lim_{x \to \infty} \frac{P^m(x) \cdot P_m(x)}{P(x)}$$

as in Corollary 6.2. Then the corollary states that

$$\#\{p < x \text{ prime } \mid a_p(f_N) \in \mathbb{Q}\} \sim \frac{1}{\alpha_N} \frac{16\sqrt{D}\widehat{F}}{3\pi^2} \frac{\sqrt{x}}{\log x}.$$

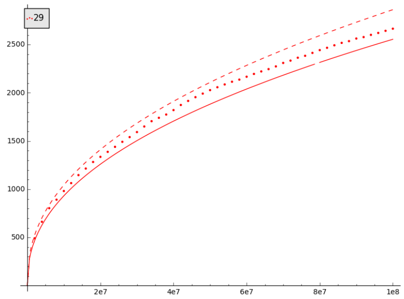
We have a convincing estimate $\widehat{c}_N$ for c_N. Moreover $\alpha_{m_N} = P^{m_N}(10^8) \cdot P_{m_N}(10^8)/P(10^8)$ is the best approximation of α_N available. So we can check this last statement by plotting both functions (Fig. 8). In this figure $1/\alpha_{m_N} \widehat{c}_N \frac{\pi(x)}{\sqrt{x}}$ clearly yields an overestimate when we in fact expect a slight underestimate. This is an indication that, although the convergence might be slow, the double limit equals 1.



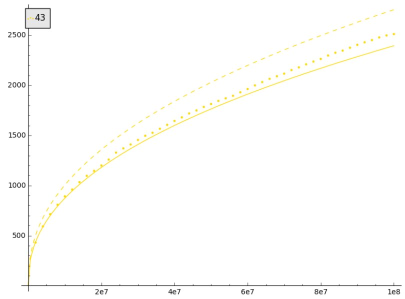
(a) $N = 29$ (b) $N = 43$ (c) $N = 55$

(d) $N = 23$ (e) $N = 87$ (f) $N = 167$

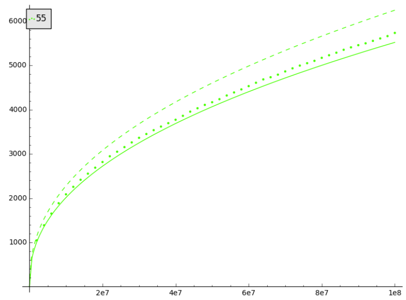
Figure 7: Plots of $P^m(x) \cdot P_m(x)/P(x)$ (dots) and the constant functions 1 (black line) and $P^{m_N}(10^8) \cdot P_{m_N}(10^8)/P(10^8)$ (coloured line) for each eigenform f_N and various divisors m of m_N for x up to 10^8.



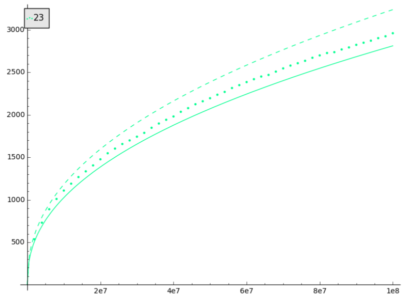
(a) $N = 29$



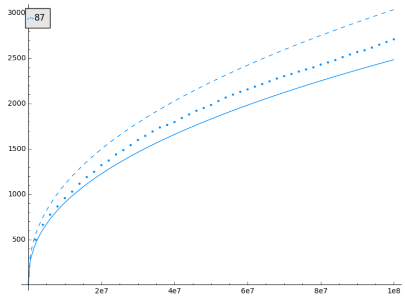
(b) $N = 43$



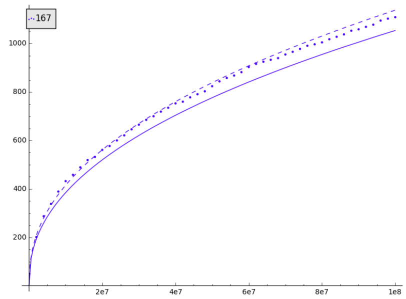
(c) $N = 55$



(d) $N = 23$



(e) $N = 87$



(f) $N = 167$

Figure 8: Plots of $\#\{p < x \text{ prime} \mid a_p \in \mathbb{Q}\}$ (dots), $\widehat{c}_N \frac{\pi(x)}{\sqrt{x}}$ (full line) and $1/\alpha_{m_N} \widehat{c}_N \frac{\pi(x)}{\sqrt{x}}$ (dashed line) for all eigenforms f_N with $\widehat{c}_N$ based on Theorem 6.3 .

A Proof of Proposition 5.6

In this appendix we give the proof of the following proposition.

Proposition 5.6. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#\mathcal{A}^t_{\ell^k,I} = \frac{(\ell-1)}{(\ell+1)}\ell^{6k-2}\left(\ell^2+\ell+1-\ell^{-2k}\right).$$

Before we give the proof we need a lemma. Let

$$\upsilon : \mathbb{Z}[\alpha] \to \mathbb{Z}$$

be the ℓ-adic valuation. By abuse of notation we will also use υ to denote the induced valuation on $\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$.

Lemma A.1. *Consider for any $k \geq r \geq 1$ the following two conditions on pairs $(a,d) \in (\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha])^2$*

$$\begin{cases} a \cdot d \in \mathbb{Z}/\ell^k\mathbb{Z}^\times + \alpha\ell^r\mathbb{Z}/\ell^k\mathbb{Z} & \text{(2a)} \\ a + d \in \mathbb{Z}/\ell^k\mathbb{Z}. & \text{(2b)} \end{cases}$$

1. *Let $b \in \mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$ with $\min\{\upsilon(b),k\} = r$. Then there exists an element $c \in \mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$ such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{A}^t_{\ell^k,I}$ if and only if both (2a) and (2b) hold. Moreover there exist precisely ℓ^{k+r} distinct such c.*
2. *There are*
$$\ell^{3k-r-2}(\ell-1)(r\ell-r+\ell)$$
pairs $(a,d) \in (\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha])^2$ satisfying (2a) and (2b).

Proof. 1. The 'only if' statement is immediate. Conversely suppose that a and d are elements of $\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$ satisfying (2a) and (2b). Let $b \in \mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$ and $k \geq r \geq 1$ with $r = \min\{\upsilon(b),k\}$. For every c in $\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$ denote

$$\sigma_c := \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Condition (2b) is equivalent with $\operatorname{tr}\sigma_c \in \mathbb{Z}/\ell^k\mathbb{Z}$. So it suffices to show that there are ℓ^{k+r} distinct c such that $\det\sigma_c \in \mathbb{Z}/\ell^k\mathbb{Z}^\times$.

Let e_1, e_2, b_1, b_2, c_1 and c_2 be elements of $\mathbb{Z}/\ell^k\mathbb{Z}$ such that

$$\begin{aligned} a \cdot d &= e_1 + \ell^r e_2\alpha, \\ b &= \ell^r(b_1 + b_2\alpha), \\ c &= c_1 + c_2\alpha. \end{aligned}$$

Then $\det \sigma_c \in \mathbb{Z}/\ell^k\mathbb{Z}^\times$ if and only if

$$e_1 - \ell^r(b_1c_1 + b_2c_2\alpha^2) \in \mathbb{Z}/\ell^k\mathbb{Z}^\times \text{ and}$$
$$\ell^r(e_2 - b_2c_1 - b_1c_2) = 0.$$

Note that (2a) implies that e_1 is invertible. So the first condition is satisfied. Moreover $\upsilon(b) \geq r$ so either b_1 or b_2 is a unit. Without loss of generality suppose that b_1 is a unit. Then $\det \sigma_c \in \mathbb{Z}/\ell^k\mathbb{Z}$ if and only if

$$c_2 \in b_1^{-1}(e_2 - b_2c_1) + \ell^{k-r}\mathbb{Z}/\ell^k\mathbb{Z}.$$

In particular there exist ℓ^{k+r} distinct such c such that $\sigma_c \in \mathcal{A}^t_{\ell^k,I}$.

2. Let a_1, a_2, d_1 and d_2 be elements of $\mathbb{Z}/\ell^k\mathbb{Z}$ such that $a = a_1 + a_2\alpha$ and $d = d_1 + d_2\alpha$. Then conditions (2a) and (2b) hold if and only if

$$\begin{cases} a_1d_1 + a_2d_2\alpha^2 \in \mathbb{Z}/\ell^k\mathbb{Z}^\times \\ a_1d_2 + a_2d_1 \in \ell^r\mathbb{Z}/\ell^k\mathbb{Z} \\ a_2 + d_2 = 0. \end{cases}$$

Using $d_2 = -a_2$ in the first expressions we obtain

$$\begin{cases} a_1d_1 - a_2^2\alpha^2 \in \mathbb{Z}/\ell^k\mathbb{Z}^\times & \text{(3a)} \\ a_2(a_1 - d_1) \in \ell^r\mathbb{Z}/\ell^k\mathbb{Z}. & \text{(3b)} \end{cases}$$

We distinguish three cases depending on the valuation of a_2.

(a) If $a_2 = 0$, then (3b) is satisfied and

$$\text{(3a)} \Leftrightarrow a_1d_1 \in \mathbb{Z}/\ell^k\mathbb{Z}^\times.$$

So there are $\ell^{2k-2}(\ell-1)^2$ such pairs (a,d).

(b) If $r \leq \upsilon(a_2) = s < k$, then $a_2 \in \ell^r\mathbb{Z}/\ell^k\mathbb{Z}$ so (3b) is satisfied and

$$\text{(3a)} \Leftrightarrow a_1d_1 \in \mathbb{Z}/\ell^k\mathbb{Z}^\times.$$

So for every $r \leq s < k$ there are $\ell^{3k-3-s}(\ell-1)^3$ pairs (a,d) with $\upsilon(a_2) = s$ that satisfy (2a) and (2b).

(c) If $0 < \upsilon(a_2) = s < r$ then

$$\begin{cases} \text{(3a)} \Leftrightarrow a_1d_1 \in \mathbb{Z}/\ell^k\mathbb{Z}^\times \\ \text{(3b)} \Leftrightarrow a_1 - d_1 \in \ell^{r-s}(\mathbb{Z}/\ell^k\mathbb{Z}^\times). \end{cases}$$

These conditions are equivalent to

$$\begin{cases} a_1 \in \mathbb{Z}/\ell^k\mathbb{Z}^\times \\ d_1 \in a_1 + \ell^{r-s}\mathbb{Z}/\ell^k\mathbb{Z}. \end{cases}$$

So for every $0 < s < r$ there are $\ell^{3k-2-r}(\ell-1)^2$ such pairs (a,d) with $\upsilon(a_2) = s$.

(d) Finally suppose that a_2 is invertible. If $a_1 \in \ell\mathbb{Z}/\ell^k\mathbb{Z}$, then (3b) implies (3a). Hence the remaining condition is

$$d_1 \in a_1 + \ell^r\mathbb{Z}/\ell^k\mathbb{Z}.$$

So there are $\ell^{3k-2-r}(\ell-1)$ pairs (a,d) with a_2 a unit and a_1 not invertible.
If a_1 is an invertible element we have

$$\begin{cases} \text{(3a)} \Leftrightarrow d_1 \notin a_1^{-1}a_2^2\alpha^2 + \ell\mathbb{Z}/\ell^k\mathbb{Z} \\ \text{(3b)} \Leftrightarrow d_1 \in a_1 + \ell^r\mathbb{Z}/\ell^k\mathbb{Z}. \end{cases}$$

Note that the intersection of $a_1^{-1}a_2^2\alpha^2 + \ell\mathbb{Z}/\ell^k\mathbb{Z}$ and $a_1 + \ell^r\mathbb{Z}/\ell^k\mathbb{Z}$ is empty. Indeed, otherwise $a_1 \equiv a_1^{-1}a_2^2\alpha^2 \mod \ell$ or $(a_1a_2^{-1})^2 \equiv \alpha^2 \mod \ell$. Which contradicts the fact that α^2 is a quadratic non-residue modulo ℓ. Hence

$$\text{(3b)} \Leftrightarrow d_1 \in a_1 + \ell^r\mathbb{Z}\ell^k\mathbb{Z} \Rightarrow \text{(3a)}.$$

In particular there are $\ell^{3k-2-r}(\ell-1)^2$ pairs (a,d) with both a_1 and a_2 invertible elements.
Adding the two cases, a_1 being a unit and a_1 not being a unit, yields

$$\begin{aligned} \ell^{3k-2-r}(\ell-1)^2 + \ell^{3k-2-r}(\ell-1) &= \ell^{3k-2-r}(\ell-1)(\ell-1+1) \\ &= \ell^{3k-1-r}(\ell-1) \end{aligned}$$

distinct pairs (a,d) satisfying (2a) and (2b) with a_1 invertible.

Finally we sum over all cases

$$\begin{aligned} &\ell^{2k-2}(\ell-1)^2 + \sum_{s=r}^{k-1} \ell^{3k-3-s}(\ell-1)^3 + \sum_{s=1}^{r-1} \ell^{3k-2-r}(\ell-1)^2 + \ell^{3k-1-r}(\ell-1) \\ &= \ell^{2k-2}(\ell-1)\Big(\ell-1+(\ell-1)\sum_{s=r}^{k-1}\ell^{k-1-s}(\ell-1) + \sum_{s=1}^{r-1}\ell^{k-r}(\ell-1) + \ell^{k-r+1}\Big). \end{aligned}$$

Note that the first summation is telescopic so the total sum yields

$$\begin{aligned} &\ell^{2k-2}(\ell-1)\Big(\ell-1+(\ell-1)(\ell^{k-r}-1) + (r-1)(\ell-1)\ell^{k-r} + \ell^{k-r+1}\Big) \\ &= \ell^{2k-2}(\ell-1)\Big(r(\ell-1)\ell^{k-r} + \ell^{k-r+1}\Big) \\ &= \ell^{3k-2-r}(\ell-1)\Big(r(\ell-1)+\ell\Big). \end{aligned}$$

□

Proof of Proposition 5.6 .
Let $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha])$. Then $\sigma \in \mathcal{A}^t_{\ell^k,I}$ if and only if

$$\begin{cases} ad - bc \in \mathbb{Z}/\ell^k\mathbb{Z}^\times & \text{(4a)} \\ a + d \in \mathbb{Z}/\ell^k\mathbb{Z}. & \text{(4b)} \end{cases}$$

We distinguish three cases depending on the valuation of b.

1. If b is a unit then

$$\begin{cases} \text{(4a)} \Leftrightarrow c \in adb^{-1} + \mathbb{Z}/\ell^k\mathbb{Z}^\times \\ \text{(4b)} \Leftrightarrow d \in -a + \mathbb{Z}/\ell^k\mathbb{Z}. \end{cases}$$

   So there are

$$\ell^{2k} \cdot \ell^{2k-2}(\ell^2 - 1) \cdot \ell^{k-1}(\ell - 1) \cdot \ell^k = \ell^{6k-3}(\ell - 1)(\ell^2 - 1)$$

   matrices $\sigma \in \mathcal{A}^t_{\ell^k,I}$ with b a unit.

2. If $b = 0$, then

$$\begin{cases} \text{(4a)} \Leftrightarrow ad \in \mathbb{Z}/\ell^k\mathbb{Z}^\times \\ \text{(4b)} \Leftrightarrow d + a \in \mathbb{Z}/\ell^k\mathbb{Z}. \end{cases}$$

   By Lemma A.1 with $r = k$ there are $\ell^{2k-2}(\ell-1)(k\ell-k+\ell)$ such pairs (a, d). Again by Lemma A.1 there are ℓ^{2k} elements c in $\mathbb{Z}_{\ell^2}$ for every such pair (a, d) so that $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$ is an element of $\mathcal{A}^t_{\ell^k,I}$. In particular we obtain

$$\ell^{4k-2}(\ell - 1)(k\ell - k + \ell)$$

   elements of $\mathcal{A}^t_{\ell^k,I}$ with $b = 0$.

3. Let $0 < v(b) = r < k$. Then by part 1 of Lemma A.1 there exists ℓ^{k+r} elements c for each b and each pair (2a) and (2b) such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{A}^t_{\ell^k,I}$. By part 2 of the same lemma there exist $\ell^{3k-2-r}(\ell - 1)(r\ell - r + \ell)$ such pairs (a, d). Moreover there are $\ell^{2k-2-2r}(\ell^2 - 1)$ elements b in $\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$ with $v(b) = r$. So there are

$$\begin{aligned} &\ell^{3k-2-r}(\ell - 1)(r\ell - r + \ell) \cdot \ell^{2k-2-2r}(\ell^2 - 1) \cdot \ell^{k+r} \\ &= \ell^{4(k-1)+2(k-r)}(\ell - 1)(\ell^2 - 1)(r\ell - r + \ell) \end{aligned}$$

   elements in $\mathcal{A}^t_{\ell^k,I}$ with $v(b) = r$ for each $0 < r < k$.

It remains to take the sum over all three cases. Note that

$$
\begin{aligned}
\#\mathcal{A}^t_{\ell^k,I} &= \ell^{6k-3}(\ell-1)(\ell^2-1) + \sum_{r=1}^{k-1} \ell^{4(k-1)+2(k-r)}(\ell-1)(\ell^2-1)(r\ell - r + \ell) \\
&\quad + \ell^{4k-2}(\ell-1)(k\ell - k + \ell) \\
&= \ell^{4(k-1)}(\ell-1)\Big(k\ell - k + \ell + \sum_{r=0}^{k} \ell^{2(k-r)}(\ell^2-1)(r(\ell-1)+\ell)\Big).
\end{aligned}
$$

We split the summation in two terms

$$
\begin{aligned}
\#\mathcal{A}^t_{\ell^k,I} =& \ell^{4(k-1)}(\ell-1)\Big(k(\ell-1) + \ell \\
&+ (\ell-1)\sum_{r=0}^{k} r\ell^{2(k-r)}(\ell^2-1) + \sum_{r=0}^{k} \ell^{2(k-r)+1}(\ell^2-1)\Big).
\end{aligned}
$$

Expand the first summation and note that the second summation is telescopic

$$
\begin{aligned}
\#\mathcal{A}^t_{\ell^k,I} =& \ell^{4(k-1)}(\ell-1)\Big(k(\ell-1) + \ell \\
&+ (\ell-1)(\ell^{2k} + \ell^{2k-2} + \cdots + \ell^2 - k) + (\ell^{2k+3} - \ell)\Big) \\
=& \ell^{4(k-1)}(\ell-1)\Big(k(\ell-1) + \ell \\
&+ (\ell-1)\frac{\ell^{2(k+1)}-1}{\ell^2-1} - (\ell-1)(1+k) + \ell^{2k+3} - \ell\Big) \\
=& \ell^{4(k-1)}(\ell-1)\Big(\frac{\ell^{2(k+1)}-1}{\ell+1} - (\ell-1) + \ell^{2k+3}\Big) \\
=& \ell^{4(k-1)}\frac{(\ell-1)}{(\ell+1)}\Big(\ell^{2(k+1)} - 1 - (\ell+1)(\ell-1) + \ell^{2k+4} + \ell^{2k+3}\Big) \\
=& \ell^{4(k-1)}\frac{(\ell-1)}{(\ell+1)}\Big(\ell^{2k+4} - \ell^2 + \ell^{2k+3} + \ell^{2k+2}\Big) \\
=& \ell^{6k-2}\frac{(\ell-1)}{(\ell+1)}\Big(\ell^2 + \ell + 1 - \ell^{-2k}\Big).
\end{aligned}
$$

□

B Proof of Proposition 5.8

In this appendix we prove Proposition 5.8.

Proposition 5.8. *Let ℓ be an odd prime and k a positive integer. Then*

$$
\#\mathcal{A}^t_{\ell^k,S} = \frac{(\ell-1)}{(\ell+1)}\ell^{6k-4}\left(\ell^4 + \ell^3 - \ell^2 - 2\ell - \ell^{-2k+2}\right).
$$

Before we prove this proposition we need three intermediate results.

Lemma B.1. *Let ℓ be an odd prime and k a positive integer. Let f be a quadratic monic polynomial in $\mathbb{Z}/\ell^k\mathbb{Z}[X]$ and D be the discriminant of f. Then*

$$\#\{r \in \mathbb{Z}/\ell^k\mathbb{Z} \mid f(r) = 0\} = \begin{cases} \ell^{\lfloor k/2 \rfloor} & \text{if } D = 0 \\ 2\ell^i & \text{if } D = u^2\ell^{2i} \text{ with } u \in \mathbb{Z}/\ell^k\mathbb{Z}^\times \text{ and } 0 \leq i \leq k/2 \\ 0 & \text{else.} \end{cases}$$

Proof. Let $f = X^2 + bX + c$ be a polynomial in $\mathbb{Z}/\ell^k\mathbb{Z}[X]$.

If f has at least one zero, say a, then

$$\begin{aligned} f(a) = 0 &\Leftrightarrow 4a^2 + 4ba + 4c = 0 \\ &\Leftrightarrow (2a + b)^2 = b^2 - 4c. \end{aligned}$$

In particular the discriminant of f is a square. Let $D = b^2 - 4c$ be the discriminant of f. We distinguish two cases based on the valuation of D.

If D is an invertible element, the result follows from Hensel's lemma. So we may assume that the valuation of D is at least one. Let $\widehat{f}$ be the reduction of f modulo ℓ. Then $\widehat{f}$ has $-b/2$ as a double zero. In particular any zero of f in $\mathbb{Z}/\ell^k\mathbb{Z}$ is of the form $-b/2 + a$ with $a \in \ell\mathbb{Z}/\ell^k\mathbb{Z}$. Let us compute

$$\begin{aligned} f\left(-\frac{b}{2} + a\right) = 0 &\Leftrightarrow (-\frac{b}{2} + a)^2 + b(-\frac{b}{2} + a) + c = 0 \\ &\Leftrightarrow \frac{b^2}{4} - \frac{b^2}{2} + c + a^2 \\ &\Leftrightarrow -\frac{D}{4} + a^2 = 0. \end{aligned}$$

If $D = 0$, the zeros of f are precisely the elements of $-\frac{b}{2} + \ell^{\lceil k/2 \rceil}\mathbb{Z}/\ell^k\mathbb{Z}$. In particular f has $\ell^{\lfloor k/2 \rfloor}$ zeros.

Finally suppose that $D = u^2\ell^{2i}$ with u an invertible element. Then the zeros of f are

$$-\frac{b}{2} \pm \frac{u}{2}\ell^i + \ell^{k-i}\mathbb{Z}/\ell^k\mathbb{Z}.$$

This set has cardinality $2\ell^i$. $\square$

For every $0 \leq i \leq k$ let P_i be the set of monic quadratic polynomials with coefficients in $\mathbb{Z}/\ell^k\mathbb{Z}$ with invertible constant term and $\min\{v(\operatorname{Disc} f), k\} = i$. Moreover consider the

following subsets of P_i

$$P_{i,0} = \left\{ f \in P_i \mid \operatorname{Disc} f \text{ not a quadratic residue in } \mathbb{Z}/\ell^k\mathbb{Z} \right\},$$
$$P_{i,2} = \left\{ f \in P_i \mid \operatorname{Disc} f \text{ a quadratic residue in } \mathbb{Z}/\ell^k\mathbb{Z} \right\},$$

where $\operatorname{Disc} f$ denotes the discriminant of the quadratic polynomial f. Note that the set $P_{i,2}$ is empty for every odd i moreover so is $P_{k,0}$ since 0 is a quadratic residue.

Lemma B.2. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#P_{i,j} = \begin{cases} \frac{(\ell-1)}{2}\ell^{2k-1} & \text{if } i = 0 \text{ and } j = 0 \\ \frac{(\ell-1)(\ell-2)}{2}\ell^{2k-2} & \text{if } i = 0 \text{ and } j = 2 \\ (\ell-1)^2\ell^{2k-2t-1} & \text{if } i = 2t-1 < k \text{ and } j = 0 \\ \frac{(\ell-1)^2}{2}\ell^{2k-2t-2} & \text{if } i = 2t < k \\ (\ell-1)\ell^{k-1} & \text{if } i = k \text{ and } j = 2 \\ 0 & \text{else.} \end{cases}$$

Proof. Let ℓ be an odd prime and k a positive integer. Let $f = X^2 + bX + c$ be a quadratic monic polynomial. We distinguish three cases depending on the valuation of the discriminant D of f.

1. Suppose that D is a unit. Then D is a square modulo $\mathbb{Z}/\ell^k\mathbb{Z}$ if and only if D is a quadratic residue modulo ℓ. So it suffices to count quadratic polynomials $f \in \mathbb{F}_\ell[X]$ with $f(0)$ a unit and D a quadratic residue or non-residue. There are $\frac{(\ell-1)\ell}{2}$ monic quadratic irreducible polynomials with $f(0) \neq 0$ in $\mathbb{F}_\ell[X]$ and $\frac{(\ell-1)(\ell-2)}{2}$ monic quadratic polynomials with $f(0) \neq 0$ and distinct roots. The result for $v(D) = 0$ follows from Hensel's lemma.

2. Let $0 < i < k$. Then
$$f \in P_i \Leftrightarrow c \in (b/2)^2 + \ell^i(\mathbb{Z}/\ell^k\mathbb{Z}^\times).$$
In particular b is a unit. For each of the $(\ell-1)\ell^{k-1}$ different choices of b, there are $(\ell-1)\ell^{k-i-1}$ choices for c. Hence $\#P_i = (\ell-1)^2\ell^{2k-i-2}$. If $i = 2t-1$ is odd, then $P_{2t-1,2}$ is empty so $\#P_{2t-1,0} = (\ell-1)^2\ell^{2k-2t-1}$. If $i = 2t$ is even then the discriminant is a square for half of the polynomials. Hence $\#P_{2t,0} = \#P_{2t,2} = \frac{(\ell-1)^2}{2}\ell^{2k-2t-2}$.

3. Finally suppose that $i = k$, then $D = 0$ if and only if $c = \frac{b^2}{4}$. Hence for every unit b there is precisely one polynomial in the set P_k with discriminant zero. □

For every non-empty set $P_{i,j}$ fix a polynomial $f_{i,j} \in P_{i,j}$. Denote

$$M_{i,j} := \{\sigma \in GL_2(\mathbb{Z}/\ell^k\mathbb{Z}) \mid \text{char. poly. } \sigma = f_{i,j}\}.$$

If no such polynomial $f_{i,j}$ exists, $M_{i,j}$ is defined as the empty set.

Lemma B.3. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#M_{i,j} = \begin{cases} (\ell-1)\ell^{2k-1} & \text{if } i=0 \text{ and } j=0 \\ (\ell+1)\ell^{2k-1} & \text{if } i=0 \text{ and } j=2 \\ (\ell^{t+1}+\ell^{t}-\ell-1)\ell^{2k-t-1} & \text{if } i=2t-1 \text{ and } j=0 \\ (\ell^{t+1}+\ell^{t}-2)\ell^{2k-t-1} & \text{if } i=2t \text{ and } j=0 \\ (\ell+1)\ell^{2k-1} & \text{if } i=2t \text{ and } j=2 \\ (\ell^{m+1}+\ell^{m}-1)\ell^{3m-1} & \text{if } i=k=2m \text{ and } j=2 \\ (\ell^{m+1}+\ell^{m}-1)\ell^{3m+1} & \text{if } i=k=2m+1 \text{ and } j=2 \\ 0 & \text{else.} \end{cases}$$

In particular $\#M_{i,j}$ does not depend on the polynomial $f_{i,j}$.

Proof. If $j=2$ and i is odd, the set $M_{i,j}$ is empty by definition and so is the set $M_{k,0}$. We prove the remaining cases.

Let ℓ be an odd prime and k a positive integer. Let $f = X^2 - TX + S \in \mathbb{Z}/\ell^k\mathbb{Z}[X]$ with S invertible. Let $D = T^2 - 4S$ be the discriminant of f. A matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has characteristic polynomial f if and only if

$$\begin{cases} d = T - a \\ a^2 - aT + S + bc = 0. \end{cases}$$

So for every pair (b,c) and every zero of $X^2 - TX + S + bc$ there exists precisely one matrix with characteristic polynomial f. By Lemma B.1 the number of zeros of $f + bc$ depends only on the discriminant of $f + bc$. The discriminant of $f + bc$ is $D - 4bc$. We distinguish three cases depending on the valuation of bc. Define

$$\begin{aligned} M_{i,j}^{<} &:= \{\sigma \in M_{i,j} \mid v(bc) < i\}, \\ M_{i,j}^{=} &:= \{\sigma \in M_{i,j} \mid \min\{v(bc), k\} = i\}, \\ M_{i,j}^{>} &:= \{\sigma \in M_{i,j} \mid \min\{v(bc), k\} > i\}. \end{aligned}$$

Then for every pair i and j

$$\#M_{i,j} = \#M_{i,j}^{<} + \#M_{i,j}^{=} + \#M_{i,j}^{>}.$$

First we compute the cardinality of each of the sets $M_{i,j}^{<}$, $M_{i,j}^{=}$ and $M_{i,j}^{>}$ for all pairs i and j.

1. Suppose that $0 \le v(bc) < \min\{v(D), k\} = i \le k$. Then $v(D - 4bc) = v(bc)$. We need only consider tuples (b,c) such that the valuation of bc is even. Indeed by Lemma

B.1 monic quadratic polynomials with odd valuated discriminant have no zeros. For each integer s with $0 \leq 2s < i$ there exist $(2s+1)(\ell-1)^2\ell^{2k-2s-2}$ pairs (b,c) such that $v(bc) = 2s$. Moreover for exactly half of these pairs $D - 4bc$ is a square. In this case there exist $2\ell^s$ solution for the polynomial $f + bc$ by Lemma B.1.

So for each $0 \leq s < \lceil i/2 \rceil - 1$ we obtain $(2s+1)(\ell-1)^2\ell^{2k-s-2}$ different matrices with characteristic polynomial f. Summing over all s yields

$$\begin{aligned}
&\sum_{s=0}^{\lceil i/2\rceil-1} (2s+1)(\ell-1)^2\ell^{2k-s-2} \\
&= 2(\ell-1)\sum_{s=0}^{\lceil i/2\rceil-1} s(\ell-1)\ell^{2k-s-2} + (\ell-1)\sum_{s=0}^{\lceil i/2\rceil-1}(\ell-1)\ell^{2k-s-2} \\
&= 2(\ell-1)\Big(\ell^{2k-2} + \ell^{2k-3} + \cdots + \ell^{2k-\lceil i/2\rceil} - (\lceil i/2\rceil - 1)\ell^{2k-\lceil i/2\rceil-1}\Big) \\
&\quad + (\ell-1)\Big(\ell^{2k-1} - \ell^{2k-\lceil i/2\rceil-1}\Big) \\
&= (\ell-1)\ell^{2k-\lceil i/2\rceil-1}\Big(2\frac{(\ell^{\lceil i/2\rceil}-1)}{\ell-1} - 2\lceil i/2\rceil + \ell^{\lceil i/2\rceil} - 1\Big) \\
&= \ell^{2k-\lceil i/2\rceil-1}\Big(2\ell^{\lceil i/2\rceil} - 2 - 2\lceil i/2\rceil(\ell-1) + \ell^{\lceil i/2\rceil}(\ell-1) - (\ell-1)\Big) \\
&= \ell^{2k-\lceil i/2\rceil-1}\Big(\ell^{\lceil i/2\rceil}(\ell+1) - 2\lceil i/2\rceil(\ell-1) - \ell - 1\Big).
\end{aligned}$$

So we obtain

$$\#M_{i,j}^{<} = \begin{cases} 0 & \text{if } i = 0 \\ \ell^{2k-\lceil i/2\rceil-1}\Big(\ell^{\lceil i/2\rceil}(\ell+1) - 2\lceil i/2\rceil(\ell-1) - \ell - 1\Big) & \text{else.}\end{cases}$$

2. Suppose that $0 \leq \min\{v(bc), k\} = i = \min\{v(D), k\} \leq k$. Then the valuation of $D - 4bc$ will be at least i and may be bigger depending on bc.

   If $i < k$ there are $(i+1)(\ell-1)^2\ell^{2k-i-2}$ pairs (b,c) such that $v(bc) = i$. Since every element of $D + \ell^i(\mathbb{Z}/\ell^k\mathbb{Z}^\times)$ occurs an equal amount of times as $D - 4bc$ for all b and c in $\mathbb{Z}/\ell^k\mathbb{Z}$ with $v(bc) = i$ it suffices to count the number of squares with given valuation. In particular each element of $D + \ell^i(\mathbb{Z}/\ell^k\mathbb{Z}^\times)$ will occur precisely

$$\begin{aligned}
\frac{\#\left\{(b,c) \in (\mathbb{Z}/\ell^k\mathbb{Z})^2 \mid v(bc) = i\right\}}{\# - D + \ell^i(\mathbb{Z}/\ell^k\mathbb{Z}^\times)} &= \frac{(i+1)(\ell-1)^2\ell^{2k-i-2}}{(\ell-1)\ell^{k-i-1}} \\
&= (i+1)(\ell-1)\ell^{k-1}
\end{aligned}$$

   times as the discriminant of $f + bc$ for all pairs (b,c) with $\min\{v(bc), k\} = i$.

   If D is not a square, then for any $i \leq 2s < k$ there are $\frac{1}{2}(\ell-1)\ell^{k-2s-1}$ squares in $D + \ell^i\mathbb{Z}/\ell\mathbb{Z}^\times$ with valuation $2s$. Each square with valuation $2s < k$ induces $2\ell^s$

distinct zeros and discriminant equal to zero induces $\ell^{\lfloor k/2 \rfloor}$ zeros. Summing over all cases yields

$$\begin{aligned}\#M_{i,0}^{=} =&(i+1)(\ell-1)\ell^{k-1}\Big(\ell^{\lfloor k/2\rfloor} + \sum_{s=\lceil i/2\rceil}^{\lceil k/2\rceil -1} \frac{(\ell-1)}{2}\ell^{k-2s-1}\cdot 2\ell^s\Big)\\ &= (i+1)(\ell-1)\ell^{k-1}\big(\ell^{\lfloor k/2\rfloor} + \ell^{k-\lceil i/2\rceil} - \ell^{k-\lceil k/2\rceil}\big)\\ &= (i+1)(\ell-1)\ell^{2k-\lceil i/2\rceil -1}.\end{aligned}$$

If D is a square, then there are only $\frac{1}{2}(\ell-3)\ell^{k-i-1}$ squares with valuation i as all elements in $D+\ell^{i+1}\mathbb{Z}/\ell^k\mathbb{Z}$ are quadratic residues modulo ℓ^k with valuation i and

$$\Big(D+\ell^{i+1}\mathbb{Z}/\ell^k\mathbb{Z}\Big) \cap \Big(D+\ell^i(\mathbb{Z}/\ell\mathbb{Z}^\times)\Big) = \varnothing.$$

The number of squares with valuation $2s > i$ is the same as in the case that D is a quadratic non-residue modulo ℓ^k. So summing over all s with $i \le 2s \le k$ yields

$$\begin{aligned}\#M_{i,2}^{=} =&(i+1)(\ell-1)\ell^{k-1}\Big(\ell^{\lfloor k/2\rfloor} + (\ell-3)\ell^{k-i/2-1} + \sum_{s=i/2+1}^{\lceil k/2\rceil -1} (\ell-1)\ell^{k-s-1}\Big)\\ &= (i+1)(\ell-1)\ell^{k-1}\big(\ell^{\lfloor k/2\rfloor} + \ell^{k-i/2} - 3\ell^{k-i/2-1} + \ell^{k-i/2-1} - \ell^{\lfloor k/2\rfloor}\big)\\ &= (i+1)(\ell-1)(\ell-2)\ell^{2k-i/2-2}.\end{aligned}$$

Finally suppose that $D = 0 = bc$. Then one checks that the number of pairs (b,c) such that $bc = 0$ is $\big((k+1)\ell-k\big)\ell^{k-1}$. For each of these pairs the discriminant of the polynomial $f+bc$ equals the discriminant of the polynomial f which is zero. In particular every pair (b,c) induces $\ell^{\lfloor k/2\rfloor}$ distinct matrices with characteristic polynomial f.

So the number of matrices with characteristic polynomial f and $0 \le \min\{v(bc),k\} = \min\{v(D),k\} = i \le k$ is

$$\#M_{i,j}^{=} = \begin{cases} (i+1)(\ell-1)(\ell-2)\ell^{2k-i/2-2} & \text{if } i<k \text{ and } j=2\\ \big((k+1)\ell-k\big)\ell^{k+\lfloor k/2\rfloor -1} & \text{if } i=k\\ (i+1)(\ell-1)\ell^{2k-\lceil i/2\rceil -1} & \text{else.}\end{cases}$$

3. Suppose that $0 \le i = v(D) < \min\{v(bc),k\} \le k$. If D is not a square in $\mathbb{Z}/\ell^k\mathbb{Z}$, then $D-4bc$ is not a square since $D-4bc \equiv D \mod \ell^{v(bc)}$ and D is a quadratic non-residue modulo $\ell^{v(bc)}$. So if D is not a square, no matrices exists.

   If D is a square with even valuation i one checks that there exists $\ell^{2k-i-2}\big((i+2)\ell - i-1\big)$ pairs (b,c) such that $i < \min\{v(bc),k\} \le k$. For each pair there exists $2\ell^{i/2}$ zeros of the polynomial $f+bc$. Hence we find

$$\#M_{i,j}^{>} = \begin{cases} 2\ell^{2k-i/2-2}\big((i+2)\ell-i-1\big) & \text{if } i<k \text{ and } j=2\\ 0 & \text{else.}\end{cases}$$

We compute the sum $\#M_{i,j} = \#M_{i,j}^{<} + \#M_{i,j}^{=} + \#M_{i,j}^{>}$ for each pair i and j.

1. Suppose that $\upsilon(D) = 0$ and D is a quadratic non-residue. Then there exist no matrices with characteristic polynomial f unless $\upsilon(bc) = 0$. In this case

$$\#M_{0,0} = (\ell - 1)\ell^{2k-1}.$$

2. If $\upsilon(D) = 0$ and D is a quadratic residue. There exist $(\ell - 1)(\ell - 2)\ell^{2k-2}$ matrices with $\upsilon(bc) = 0$ and $2\ell^{2k-2}(2\ell - 1)$ with $\upsilon(bc) > 0$. Hence we obtain

$$\#M_{0,2} = (\ell + 1)\ell^{2k-1}.$$

3. If $0 < i < k$ is odd, say $i = 2t - 1$. Then

$$\begin{aligned}\#M_{2t-1,0} =& \ell^{2k-t-1}\Big(\ell^t(\ell + 1) - 2t(\ell - 1) - \ell - 1\Big) + 2t(\ell - 1)\ell^{2k-t-1}\\ &= (\ell^{t+1} + \ell^t - \ell - 1)\ell^{2k-t-1}.\end{aligned}$$

4. If i is even say $i = 2t$ and D is not a square. We obtain

$$\begin{aligned}\#M_{2t,0} &= \ell^{2k-t-1}\big(\ell^t(\ell + 1) - 2t(\ell - 1) - \ell - 1\big) + (2t + 1)(\ell - 1)\ell^{2k-t-1}\\ &= (\ell^{t+1} + \ell^t - 2)\ell^{2k-t-1}.\end{aligned}$$

5. If $i = 2t$ and D is a square. Then summing over all cases yields

$$\begin{aligned}\#M_{2t,2} &= \ell^{2k-t-1}\big(\ell^t(\ell + 1) - 2t(\ell - 1) - \ell - 1\big)\\ &+ \ell^{2k-t-2}(2t + 1)(\ell - 1)(\ell - 2) + 2\ell^{2k-t-2}\big((2t + 2)\ell - 2t - 1\big)\\ &= (\ell + 1)\ell^{2k-1}.\end{aligned}$$

6. If $D = 0$ and $k = 2m$. We obtain

$$\begin{aligned}\#M_{k,2} &= \ell^{4m-m-1}\big(\ell^m(\ell + 1) - 2m(\ell - 1) - \ell - 1\big)\\ &+ \ell^{2m+m-1}\big((2m + 1)\ell - 2m\big)\\ &= \ell^{3m-1}(\ell^{m+1} + \ell^m - 1).\end{aligned}$$

7. If $D = 0$ and $k = 2m + 1$. Then

$$\begin{aligned}\#M_{k,2} &= \ell^{4m+2-m-1-1}\big(\ell^{m+1}(\ell + 1) - 2(m + 1)(\ell - 1) - \ell - 1\big)\\ &+ \ell^{2m+1+m-1}\big((2m + 2)\ell - 2m - 1\big)\\ &= \ell^{3m+1}(\ell^{m+1} + \ell^m - 1).\end{aligned}$$

In particular the cardinality of $M_{i,j}$ does not depend on the choice of $f_{i,j}$. $\square$

Proof of Proposition 5.8. Recall that

$$\mathcal{A}^t_{\ell^k,S} = \{(\tau,\tau') \in GL_2(\mathbb{Z}/\ell^k\mathbb{Z})^2 \mid \text{char. poly. } \tau = \text{char. poly. } \tau'\}.$$

So

$$\begin{aligned}\#\mathcal{A}^t_{\ell^k,S} &= \sum_{f\in\mathbb{Z}/\ell^k\mathbb{Z}[X]} \big(\#\{\tau \in GL_2(\mathbb{Z}/\ell^k\mathbb{Z}) \mid \text{char. poly. } \tau = f\}\big)^2 \\ &= \sum_{i,j} \#P_{i,j}\cdot(\#M_{i,j})^2\end{aligned}$$

where the sum is taken over all pairs (i,j) with $0\le i<k$ and $j=0,2$ and the pair $(i,j)=(k,2)$. The factors $\#P_{i,j}$ and $\#M_{i,j}$ are computed in Lemmas B.2 and B.3 respectively. We will only give the proof if k is odd. If k is even the computation is similar. Suppose that $k=2m+1$. Then

$$\begin{aligned}\#\mathcal{A}^t_{\ell^k,S} =& \frac{(\ell-1)}{2}\ell^{2k-1}\cdot(\ell-1)^2\ell^{4k-2} + \frac{(\ell-1)(\ell-2)}{2}\ell^{2k-2}\cdot(\ell+1)^2\ell^{4k-2} \\ &+\sum_{t=1}^m\Big((\ell-1)^2\ell^{2k-2t-1}\cdot\big(\ell^t(\ell+1)-(\ell+1)\big)^2\ell^{4k-2t-2} \\ &+\frac{(\ell-1)^2}{2}\ell^{2k-2t-2}\cdot\big(\ell^t(\ell+1)-2\big)^2\ell^{4k-2t-2} \\ &+\frac{(\ell-1)^2}{2}\ell^{2k-2t-2}\cdot(\ell+1)^2\ell^{4k-2}\Big) \\ &+(\ell-1)\ell^{2m}\cdot\big(\ell^m(\ell+1)-1\big)^2\ell^{6m+2} \\ =&\frac{(\ell-1)}{2}\ell^{6k-4}\big((\ell-1)^2\ell+(\ell+1)^2(\ell-2)\big) \\ &+\sum_{t=1}^m\ell^{6k-4t-4}\Bigg(\frac{(\ell-1)^2}{2}\big(2\ell^{2t+1}(\ell+1)^2-4\ell^{t+1}(\ell+1)^2+2\ell(\ell+1)^2\big) \\ &+\frac{(\ell-1)^2}{2}\big(\ell^{2t}(\ell+1)^2-4\ell^t(\ell+1)+4\big) \\ &+\frac{(\ell-1)^2}{2}\ell^{2t}(\ell+1)^2\Bigg) \\ &+(\ell-1)\ell^{8m+2}\big(\ell^{2m}(\ell+1)^2-2\ell^m(\ell+1)+1\big) \\ =&\frac{(\ell-1)}{2}\ell^{6k-4}(2\ell^3-2\ell^2-2\ell-2) \\ &+\frac{(\ell-1)^2}{2}\sum_{t=1}^m\ell^{6k-4t-4}\Big(2\ell^{2t}(\ell+1)^3-4\ell^t(\ell+1)(\ell^2+\ell+1)+2(\ell^2+1)(\ell+2)\Big) \\ &+(\ell-1)\big((\ell+1)^2\ell^{10m+2}-2(\ell+1)\ell^{9m+2}+\ell^{8m+2}\big).\end{aligned}$$

Splitting the summation into three sums yields

$$\begin{aligned}\#\mathcal{A}^t_{\ell^k,S} =&(\ell-1)\ell^{6k-4}(\ell^3-\ell^2-\ell-1)\\&+(\ell-1)(\ell+1)^2\sum_{t=1}^{m}(\ell^2-1)\ell^{6k-2t-4}\\&-2(\ell-1)(\ell+1)\sum_{t=1}^{m}(\ell^3-1)\ell^{6k-3t-4}\\&+\frac{(\ell-1)(\ell+2)}{(\ell+1)}\sum_{t=1}^{m}(\ell^4-1)\ell^{6k-4t-4}\\&+(\ell-1)\big((\ell+1)^2\ell^{10m+2}-2(\ell+1)\ell^{9m+2}+\ell^{8m+2}\big).\end{aligned}$$

Computing the telescopic sums and using that $k=2m+1$

$$\begin{aligned}\#\mathcal{A}^t_{\ell^k,S} =&(\ell-1)\ell^{12m+2}(\ell^3-\ell^2-\ell-1)\\&+(\ell-1)(\ell+1)^2(\ell^{12m+2}-\ell^{10m+2})\\&-2(\ell-1)(\ell+1)(\ell^{12m+2}-\ell^{9m+2})\\&+\frac{(\ell-1)(\ell+2)}{(\ell+1)}(\ell^{12m+2}-\ell^{8m+2})\\&+(\ell-1)\big((\ell+1)^2\ell^{10m+2}-2(\ell+1)\ell^{9m+2}+\ell^{8m+2}\big).\end{aligned}$$

By sorting the powers of ℓ^m we obtain

$$\begin{aligned}\#\mathcal{A}^t_{\ell^k,S} =&(\ell-1)\ell^{12m+2}\Big((\ell^3-\ell^2-\ell-1)+(\ell+1)^2-2(\ell+1)+\frac{(\ell+2)}{(\ell+1)}\Big)\\&+(\ell-1)(\ell+1)^2\ell^{10m+2}(-1+1)\\&-2(\ell-1)(\ell+1)\ell^{9m+2}(-1+1)\\&+(\ell-1)\ell^{8m+2}\Big(-\frac{(\ell+2)}{(\ell+1)}+1\Big)\\=&(\ell-1)\ell^{12m+2}\Big(\ell^3-\ell-2+\frac{(\ell+2)}{(\ell+1)}\Big)-\frac{(\ell-1)}{(\ell+1)}\ell^{8m+2}\\=&\frac{(\ell-1)}{(\ell+1)}\ell^{12m+2}(\ell^4+\ell^3-\ell^2-2\ell-\ell^{-4m}).\end{aligned}$$

Using that $k=2m+1$ yields

$$\#\mathcal{A}^t_{\ell^k,S} =\frac{(\ell-1)}{(\ell+1)}\ell^{6k-4}(\ell^4+\ell^3-\ell^2-2\ell-\ell^{-2k+2}). \qquad \square$$

References

[1] Peter R. Bending. Curves of genus 2 with $\sqrt{2}$ multiplication. 1999.

[2] Nicolas Billerey and Luis V. Dieulefait. Explicit large image theorems for modular forms. *J. Lond. Math. Soc. (2)*, 89(2):499–523, 2014.

[3] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*, pages 2–140. Int. Press, Cambridge, MA, 1997.

[4] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[5] Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland. Sato-Tate distributions and Galois endomorphism modules in genus 2. *Compos. Math.*, 148(5):1390–1442, 2012.

[6] Christian Johansson. On the Sato-Tate conjecture for non-generic abelian surfaces. *arXiv:1307.6478v5*, 2015.

[7] Kiran S. Kedlaya and Andrew V. Sutherland. Computing L-series of hyperelliptic curves. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 312–326. Springer, Berlin, 2008.

[8] Koopa Tak-Lun Koo, William Stein, and Gabor Wiese. On the generation of the coefficient field of a newform by a single Hecke eigenvalue. *J. Théor. Nombres Bordeaux*, 20(2):373–384, 2008.

[9] Serge Lang. *Introduction to modular forms*, volume 222 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1995. With appendixes by D. Zagier and Walter Feit, Corrected reprint of the 1976 original.

[10] Serge Lang and Hale Trotter. *Frobenius distributions in* GL_2*-extensions.* Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers.

[11] D. Loeffler. Images of adelic Galois representations for modular forms. *ArXiv e-prints*, November 2014.

[12] V. Kumar Murty. Frobenius distributions and Galois representations. In *Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996)*, volume 66 of *Proc. Sympos. Pure Math.*, pages 193–211. Amer. Math. Soc., Providence, RI, 1999.

[13] K. A. Ribet. Endomorphism algebras of abelian varieties attached to newforms of weight 2. In *Seminar on Number Theory, Paris 1979–80*, volume 12 of *Progr. Math.*, pages 263–276. Birkhäuser, Boston, Mass., 1981.

[14] Kenneth A. Ribet. On l-adic representations attached to modular forms. *Invent. Math.*, 28:245–275, 1975.

[15] Kenneth A. Ribet. Twists of modular forms and endomorphisms of abelian varieties. *Math. Ann.*, 253(1):43–62, 1980.

[16] Jean-Pierre Serre. Un critère d'indépendance pour une famille de représentations ℓ-adiques. *Comment. Math. Helv.*, 88(3):541–554, 2013.

[17] W. A. Stein et al. *Sage Mathematics Software (Version 6.3)*. The Sage Development Team, 2014. `http://www.sagemath.org`.

[18] John Wilson. Explicit moduli for curves of genus 2 with real multiplication by $\mathbb{Q}(\sqrt{5})$. *Acta Arith.*, 93(2):121–138, 2000.

KU Leuven
Department of Mathemetics
Celestijnenlaan 200 B
B-3001 Heverlee
BELGIUM

Université du Luxembourg
Mathematics Research Unit FSTC
6, rue Richard Coudenhove-Kalergi
L-1359 Luxembourg
LUXEMBOURG

`jasper.vanhirtum@wis.kuleuven.be`